LEWIS BRISBOIS BISGAARD & SMITH LLP
ATTORNEYS AT LAW

550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Telephone: 215.977.4100
Fax: 215.977.4101
www.lewisbrisbois.com

JAMES E. PRENDERGAST
DIRECT DIAL: 215.977.4058
JIM.PRENDERGAST@LEWISBRISBOIS.COM

July 23, 2015

VIA U.S. MAIL
Iowa Attorney General
Consumer Protection Division
1305 E. Walnut Street
Des Moines, IA 50319

Re: Supplemental Notice of Data Security Event

To Whom It May Concern:

We represent Medical Informatics Engineering and NoMoreClipboard, a wholly owned subsidiary of Medical Informatics Engineering, 6302 Constitution Drive, Fort Wayne, Indiana 46804 (our "Client"). We are writing to *supplement* our notice previously sent to your office on June 19, 2015 of a data security event involving personal information of certain Iowa residents that are affiliated with certain Medical Informatics Engineering and NoMoreClipboard clients. A copy of this prior notice is attached to this letter as ***Exhibit A***.

Attached as ***Exhibit B*** is a list identifying the Medical Informatics Engineering and NoMoreClipbaord clients affected by this data security event. ***Exhibit B*** includes certain covered entities that may not be required to report given the scope of the data security event. These entities have been included in this supplemental notice out of an abundance of caution, and in the interest of prompt notification to affected individuals. This supplemental notice does not constitute an acknowledgement by the covered entities identified in ***Exhibit B*** that Iowa law requires notification or that the covered entities waive any preemption of Iowa law that may apply under state or federal law. Additionally, by providing this supplemental notice, our Client does not waive any rights or defenses regarding the applicability of Iowa law or personal jurisdiction.

Investigation Update

Our Client is currently conducting an extensive forensic investigation to determine the information affected by this incident. While this investigation is ongoing, Medical Informatics Engineering determined that the personal and protected health information affected by this incident relates to individuals affiliated with certain Medical Informatics Engineering clients and may include the individuals' name, mailing address, username, hashed password, security question and answer, email address, date of birth, Social Security number, lab results, doctor's name, health insurance policy information, diagnosis, disability code, medical conditions, telephone number, spousal information

(name and potentially date of birth), child's name and birth statistics. The information relating to affected NoMoreClipboard accounts includes personal and protected health information such as an individuals' name, home address, Social Security number, username, hashed password, security question and answer, email address, date of birth, health information, health insurance policy information, and spousal information (name and potentially date of birth).

Notice to Iowa Residents

Although our Client's investigation and law enforcement's criminal investigation into this data security event are ongoing, our Client began mailing notice letters to affected individuals for whom it has valid mailing addresses on July 17, 2015 in substantially the same form as the letters attached as ***Exhibit C***. On July 23, 2015, our client will also supplement the June 10, 2015 website notice posted on Medical Informatics Engineering and NoMoreClipboard's dedicated websites (www.mieweb.com and www.nomoreclipboard.com) and issue a national supplemental press release to major statewide media. Attached as ***Exhibit D*** is a copy of the supplemental website notice and the supplemental press release.

To date, our Client has identified seven thousand two hundred fifty-two (7,252) Iowa residents affected by this data security event.

Other Steps Taken

Medical Informatics Engineering and NoMoreClipboard take this matter, and the security of the personal and protected health information in its care, seriously and are taking measures to restore the secure functionality of the affected systems. Upon discovering this data security compromise, Medical Informatics Engineering and NoMoreClipboard took steps to identify and remediate potential vulnerabilities with its systems. Although the affected systems were remediated on June 2, 2015 and restored to secure functionality, Medical Informatics Engineering and NoMoreClipboard continue to work closely with the third-party experts to enhance the security of its systems. Remedial efforts in this matter include removing the capabilities used by the intruder to gain unauthorized access to the Medical Informatics Engineering and NoMoreClipboard affected systems, enhancing and strengthening password rules and storage mechanisms, increasing active monitoring of the affected systems, and participating in intelligence exchange with law enforcement. Medical Informatics Engineering and NoMoreClipboard have also instituted a universal password reset for all affected accounts.

To support potentially affected individuals, Medical Informatics Engineering and NoMoreClipboard established a toll-free hotline on June 10, 2015, to answer questions about this incident and to provide information relating to protection against identity theft and fraud. Medical Informatics Engineering and NoMoreClipboard provided affected individuals access to a two-year membership to credit monitoring and identity protection services through Experian, at no cost to the affected individual. Medical Informatics Engineering and NoMoreClipboard are also working closely with affected clients to ensure affected individuals are notified of this incident.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security compromise, please contact me at 215-977-4058 or Sian Schafle at 215-977-4067.

Very truly yours,

James E. Prendergast of
LEWIS BRISBOIS BISGAARD & SMITH LLP

SMS:JEP
Encl.

EXHIBIT A

LEWIS BRISBOIS BISGAARD & SMITH LLP
ATTORNEYS AT LAW

550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Telephone: 215.977.4100
Fax: 215.977.4101
www.lewisbrisbois.com

JAMES E. PRENDERGAST
DIRECT DIAL: 215.977.4058
JIM.PRENDERGAST@LEWISBRISBOIS.COM

June 19, 2015

VIA U.S. MAIL
Iowa Attorney General
Consumer Protection Division
1305 E. Walnut Street
Des Moines, IA 50319

Re: Preliminary Notice of Data Security Event

To Whom It May Concern:

We represent Medical Informatics Engineering and NoMoreClipboard, a wholly owned subsidiary of Medical Informatics Engineering, 6302 Constitution Drive, Fort Wayne, Indiana 46804, and are writing to notify you of a data security incident that may have compromised the security of personal information of an as yet unconfirmed number of Iowa residents.

Medical Informatics Engineering is a third-party provider that provides electronic medical record services to healthcare providers. NoMoreClipboard provides personal health record/patient portals sponsored by healthcare providers. The affected Iowa residents include patients affiliated with certain Medical Informatics Engineering and NoMoreClipboard clients. Medical Informatics Engineering and NoMoreClipboard provided notice of this incident to affected clients on June 2, 2015 in substantially the same form as the letter attached as *Exhibit A*.

Medical Informatics Engineering and NoMoreClipboard's investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Medical Informatics Engineering and NoMoreClipboard do not waive any rights or defenses regarding the applicability of Iowa law or personal jurisdiction.

Nature of the Data Security Event

On May 26, 2015, Medical Informatics Engineering discovered suspicious activity in one of its servers. Medical Informatics Engineering immediately began an investigation to identify and remediate any identified security vulnerability. Medical Informatics Engineering is working with a team of third-party experts to investigate the attack and enhance data security and protection. On May 26, 2015, Medical Informatics Engineering also reported this incident to law enforcement including the FBI Cyber Squad. Law enforcement is actively investigating this matter, and Medical Informatics Engineering is

cooperating fully with law enforcement's investigation. The investigation indicates this is a sophisticated cyber attack.

While investigations into this incident are ongoing, Medical Informatics Engineering determined the security of some personal and protected health information contained on Medical Informatics Engineering's network has been affected. The personal and protected health information affected by this incident may include the following information relating to individuals affiliated with certain Medical Informatics Engineering clients: name, mailing address, email address, date of birth, and for some individuals a Social Security number, lab results, dictated reports, and medical conditions. The personal and protected health information affected by this incident relating to affected NoMoreClipboard accounts may include the following information: name, home address, username, hashed password, security question and answer, email address, date of birth, health information, insurance policy information, and Social Security number. No financial or credit card information has been compromised by this incident, as Medical Informatics Engineering and NoMoreClipboard do not collect or store this information.

Notice to Affected Iowa Residents

Medical Informatics Engineering and NoMoreClipboard are working to identify the affected Iowa residents. While this investigation and law enforcement's investigations continue, Medical Informatics Engineering and NoMoreClipboard are taking appropriate steps to notify individuals potentially affected by this incident. In addition to notifying affected healthcare clients on June 2, 2015, on June 10, 2015, Medical Informatics Engineering and NoMoreClipboard began notifying the public of this security compromise. This notice was posted on Medical Informatics Engineering and NoMoreClipboard's dedicated websites (www.mieweb.com and www.nomoreclipboard.com). A copy of these statements is attached as *Exhibit B*. Notice of this incident was also distributed by way of press release to major statewide media on June 10, 2015 in substantially the same form as the statement attached here as *Exhibit C*.

We anticipate that the forensics analysis will be completed shortly. Once the analysis is complete, we will verify the total number of affected individuals, as well as the state of residence for each.

This notice to the Iowa Office of the Attorney General will be supplemented accordingly at that time.

Once the third party forensics expert's analysis is complete and the number of affected Iowa residents has been confirmed, notice letters will be mailed to the Iowa residents for whom Medical Informatics Engineering and NoMoreClipboard have valid mailing addresses pursuant to Iowa's data breach notification law. We will also supplement this preliminary notice to your office to provide an update on this data security compromise, the mailing date of notice to the affected Iowa residents, and a copy of the notification template that will be used to notify these residents.

Other Steps Taken and To be Taken

Medical Informatics Engineering and NoMoreClipboard take this matter, and the security of the personal and protected health information in its care, seriously and are taking measures to restore the secure functionality of the affected systems. Upon discovering this data security compromise, Medical

Informatics Engineering and NoMoreClipboard took steps to identify potential vulnerabilities with its systems, remediate, and enhance the security of its systems. Medical Informatics Engineering and NoMoreClipboard continue to work closely with the third-party experts to identify the nature and scope of this incident and to remediate accordingly. Remedial efforts include removing the capabilities used by the intruder to gain unauthorized access to the Medical Informatics Engineering and NoMoreClipboard affected systems, enhanced and strengthened password rules and storage mechanisms, increased active monitoring of the affected systems, and participating in intelligence exchange with law enforcement. While remediation occurs, Medical Informatics Engineering and NoMoreClipboard have instituted a universal password reset for all affected accounts.

To support potentially affected individuals, Medical Informatics Engineering and NoMoreClipboard established a toll-free hotline to answer questions about this incident and to provide information relating to protection against identity theft and fraud. Medical Informatics Engineering and NoMoreClipboard will provide affected individuals access to a two-year membership to credit monitoring and identity protection services through Experian, at no cost to the affected individual. Medical Informatics Engineering and NoMoreClipboard are also working closely with affected clients to ensure affected individuals are notified of this incident.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security compromise, please contact me at 215-977-4058 or Sian Schafle at 215-977-4067.

Very truly yours,

James E. Prendergast of
LEWIS BRISBOIS BISGAARD & SMITH LLP

SMS:JEP
Encl.

EXHIBIT A

Notice of Medical Informatics Engineering Data Incident

HIPAA Covered Entity:	[name of covered entity]
Number of Individuals:	To be determined
Notice Date:	June 1, 2015
Medical Informatics Engineering Contact:	[name, Title], [telephone number]

Medical Informatics Engineering ("MIE") is writing to provide notice of a data security compromise that may have affected the security of some protected health information contained on our network, relating to certain [client name] patients. We ask that you provide this correspondence to appropriate administrative and/or managerial staff at your company to ensure this incident is brought to the attention of all necessary members of your organization.

On May 26, 2015, the technical team at MIE discovered suspicious activity relating to one of our servers. We immediately initiated our Incident Response Plan and commenced an investigation to identify and remediate any identified security vulnerability. Our team, including independent third-party forensics experts, has been working continuously to understand the nature and scope of the incident and to confirm the security of our systems. This investigation is ongoing. On May 26, 2015, we also reported this incident to the FBI Cyber Squad, and are cooperating with the FBI's investigation.

While our investigation and law enforcement's investigation into this incident are ongoing, we determined that some protected health information contained on our network relating to a soon to be confirmed number of patients was exposed as a result of this incident. The affected data may include patient name, home address, email address, date of birth, and for some patients a Social Security number. Other protected health information affected by this incident may include lab results, dictated reports and medical conditions. Our forensic investigation indicates the unauthorized access to our network occurred on May 7, 2015 through May 8, 2015. The attackers regained unauthorized accessed to our network on May 25, 2015.

We take the security of your patients' information very seriously, and apologize for any concern and inconvenience this may cause you or your patients. Certain legal duties may exist as a result of this exposure, and we would like to assist you in satisfying these duties.

Under applicable law, you may be required to provide notice of this incident to your patients, as well as certain federal and state regulators, and/or the national consumer reporting agencies. We retained Lewis Brisbois Bisgaard & Smith, LLP ("LBBS") to assist us in determining what legal obligations may exist as a result of this incident.

Your company's precise notice obligations, and the time in which you may be required to satisfy such obligations, are determined by HIPAA and potentially various states' laws. Based on your risk assessment, the incident may require you to report details to the U.S. Department of Health and Human Services ("HHS") and to the [client name] patients whose information was contained on our network at the time of the attack. Notification duties to affected individuals, state regulators and the national consumer reporting agencies may also be required under the data breach notification laws of the states where your patients reside. This notice does not constitute legal or compliance advice.

Should you require specific legal guidance, we encourage you to discuss the contents of this letter, and MIE's proposed actions, with independent legal counsel. If you wish to provide notice of this incident to your patients directly, we encourage you to consult legal counsel. LBBS would be happy to discuss this matter with your legal counsel.

We would like to provide notice of this incident, on your company's behalf, to your affected patients, the national consumer reporting agencies, HHS, and applicable State Attorneys General. Attached as ***Exhibit A*** is a list of the regulators MIE will notify regarding this incident. We are notifying only the regulators identified in ***Exhibit A***. If your company has reporting obligations to other regulators, including the California Department of Public Health, that notice will be have to be submitted directly by your company. If you would like MIE to provide notice of this incident to your affected patients, the national consumer reporting agencies, and the regulators identified in ***Exhibit A***, please confirm that we have your authority to provide these notices as soon as possible but, because time is of the essence, no later than [DATE]. **[FOR applicable clients requiring system review: <u>We also need your authority to access your company's data contained on our network to determine the identity of the affected [client name] patients and the precise protected health information relating to these individuals that has been affected by this incident</u>]**. Consent to provide these notices on your company's behalf may be sent to [Eric Jones contact information].

We take the security of protected health information very seriously. With your authorization, in addition to mailing notice to your affected patients, we will also provide your affected patients with the opportunity to enroll in identity monitoring and protection services at no cost to them should they feel it is appropriate to do so.

We will establish a toll-free number that individuals can call if they have any questions regarding this incident. That number will be provided in the notices to affected individuals.

We are continuing to investigate this incident, and we are working diligently to address any identified security vulnerability associated with this incident. We are also reviewing our security practices to enhance the security of protected health information at MIE.

All questions regarding this notice and questions regarding the provision of mailing addresses should be directed to our privacy and data security counsel, James Prendergast at (215) 977-4067.

Our investigation into this incident is ongoing. We will update you with any substantial developments in this matter. We remain committed to the privacy of protected health information, and sincerely regret any inconvenience or concern that this may have caused you.

Sincerely,

[signatory]
[title]

Notice of Medical Informatics Engineering Data Incident

HIPAA Covered Entity:	[name of covered entity]
Number of Individuals Impacted:	To be determined
Notice Date:	June 1, 2015
NMC/Medical Informatics Engineering Contact:	[name, Title], [telephone number]

NoMoreClipboard ("NMC") is writing to provide notice of a data security compromise that may have affected the security of some protected health information relating to certain individuals who used a NMC patient portal/personal health record sponsored by your organization. We ask that you provide this correspondence to appropriate administrative and/or managerial staff at your company to ensure this incident is brought to the attention of all necessary members of your organization.

On May 26, 2015, the technical team at our parent company (Medical Informatics Engineering) discovered suspicious activity relating to one of its servers. We immediately initiated our Incident Response Plan and commenced an investigation to identify and remediate any identified security vulnerability. Our team, including independent third-party forensics experts, has been working continuously to understand the nature and scope of the incident and to confirm the security of our systems. This investigation is ongoing. On May 26, 2015, we also reported this incident to the FBI Cyber Squad, and are cooperating with the FBI's investigation.

While our investigation and law enforcement's investigation into this incident are ongoing, we determined that some protected health information contained on our network, including information relating to a soon to be confirmed number of individuals who used a NMC portal sponsored by your organization, was exposed as a result of this incident. The affected data may include patient name, home address, email address, date of birth and Social Security number. No financial or credit card information was compromised, as we do not collect or store this information. Our forensic investigation indicates the unauthorized access to our network occurred on May 7, 2015 through May 8, 2015. The attackers regained unauthorized accessed to our network on May 25, 2015.

[Our investigation thus far indicates that patient records from your Medical Informatics Engineering electronic health record have not been compromised.]

Comment [SS1]: For NMC clients who also have MIE eHR

We take the security of your patients' information very seriously, and apologize for any concern and inconvenience this may cause you or your patients. Certain legal duties may exist as a result of this exposure, and we would like to assist you in satisfying these duties.

Under applicable law, you may be required to provide notice of this incident to your patients, as well as certain federal and state regulators, and/or the national consumer reporting agencies. We retained Lewis Brisbois Bisgaard & Smith, LLP ("LBBS") to assist us in determining what legal obligations may exist as a result of this incident.

Your company's precise notice obligations, and the time in which you may be required to satisfy such obligations, are determined by HIPAA and potentially various states' laws. Based on your

risk assessment, the incident may require you to report details to the U.S. Department of Health and Human Services ("HHS") and to the [client name] patients whose information was contained on our network at the time of the attack. Notification duties to affected individuals, state regulators and the national consumer reporting agencies may also be required under the data breach notification laws of the states where your patients reside. This notice does not constitute legal or compliance advice.

Should you require specific legal guidance, we encourage you to discuss the contents of this letter, and NMC's proposed actions, with legal counsel. If you wish to provide notice of this incident to your patients directly, we encourage you to consult legal counsel. LBBS would be happy to discuss this matter with your legal counsel.

NMC would like to provide notice of this incident, on your company's behalf, to your affected patients, the national consumer reporting agencies, HHS, and applicable State Attorneys General. Attached as ***Exhibit A*** is a list of the regulators NMC will notify regarding this incident. We are notifying only the regulators identified in ***Exhibit A***. If your company has reporting obligations to other regulators, including the California Department of Public Health, that notice will have to be submitted directly by your company. If you would like NMC to provide notice of this incident to your affected patients, the national consumer reporting agencies, and the regulators identified in ***Exhibit A***, please confirm that we have your authority to provide these notices as soon as possible but, because time is of the essence, no later than **Friday, June 12, 2015.** Consent to provide these notices on your company's behalf may be sent to [Eric Jones contact information].

NMC takes the security of protected health information very seriously. With your authorization, in addition to mailing notice to your affected patients, we will also provide your affected patients with the opportunity to enroll in identity monitoring and protection services at no cost to them should they feel it is appropriate to do so.

We will establish a toll-free number that individuals can call if they have any questions regarding this incident. That number will be provided in the notices to affected individuals.

We are continuing to investigate this incident, and we are working diligently to address any identified security vulnerability associated with this incident. We are also reviewing our security practices to enhance the security of protected health information at NMC.

All questions regarding this notice and questions regarding the provision of mailing addresses should be directed to our privacy and data security counsel, James Prendergast at (215) 977-4067.

Our investigation into this incident is ongoing. We will update you with any substantial developments in this matter. We remain committed to the privacy of protected health information, and sincerely regret any inconvenience or concern that this may have caused you. .

EXHIBIT B

Medical Informatics Engineering Notifies
Individuals of a Data Security Compromise

Fort Wayne, Indiana, June 10, 2015 – On behalf of itself and its affected clients, Medical Informatics Engineering is writing to provide notice of a data security compromise that has affected the security of some protected health information relating to certain patients affiliated with certain Medical Informatics Engineering clients. *We emphasize that the patients of only certain clients of Medical Informatics Engineering were affected by this compromise and those clients have all been notified.* Clients include: Concentra, Fort Wayne Neurological Center, Franciscan St. Francis Health Indianapolis, Gynecology Center, Inc. Fort Wayne, and Rochester Medical Group.

On May 26, 2015, Medical Informatics Engineering discovered suspicious activity relating to one of its servers. Medical Informatics Engineering immediately began an investigation to identify and remediate any identified security vulnerability. Medical Informatics Engineering's team, including independent third-party forensics experts, has been working continuously to investigate the attack and enhance data security and protection. On May 26, 2015, Medical Informatics Engineering also reported this incident to law enforcement including the FBI Cyber Squad. Law enforcement is actively investigating this matter, and Medical Informatics Engineering is cooperating with law enforcement's investigation. Medical Informatics Engineering's forensic investigation indicates the unauthorized access to our network began on May 7, 2015. The investigation indicates this is a sophisticated cyber attack.

Compromised information

While investigations into this incident are ongoing, Medical Informatics Engineering determined the security of some protected health information contained on Medical Informatics Engineering's network has been affected. The protected health information affected by this incident relates to patients affiliated with certain Medical Informatics Engineering clients identified above and may include the patients' name, mailing address, email address, date of birth, and for some patients a social security number, lab results, dictated reports, and medical conditions. No financial or credit card information has been compromised, as we do not collect or store this information.

Medical Informatics Engineering also determined that this cyber attack compromised protected health information for its NoMoreClipboard subsidiary. Separate notice is being issued for affected clients and patients associated with NoMoreClipboard.

Notification

On June 2, 2015, Medical Informatics Engineering began contacting and mailing notice letters disclosing this incident to affected Medical Informatics Engineering clients.

Affected patients for whom Medical Informatics Engineering has a valid postal address will be notified of this incident through U.S. mail. Medical Informatics Engineering will also be disclosing this incident to certain state and federal regulators.

Identity protection services

As the investigations continue, and out of an abundance of caution, Medical Informatics Engineering is offering credit monitoring and identity protection services to affected patients, free of charge, for the next 24 months.

Medical Informatics Engineering has established a toll-free call center to answer questions relating to this data security event and the support and services being provided.

Fraud prevention tips

Medical Informatics Engineering suggests that affected patients remain vigilant and seek to protect against possible identity theft or other financial loss by reviewing account statements, notifying their credit card companies, healthcare providers, and insurers of the data compromise, and monitoring their credit reports. Affected patients may also review Explanation of Benefits statements for irregularities. If an individual does not receive regular Explanation of Benefits statements, he or she can contact his or her health plan and request them to send such statements following the provision of services.

Under U.S. law, patients are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, visit www.annualcreditreport.com or call, toll-free, (877) 322-8228.

At no charge, potentially affected patients can also have these credit bureaus place a "fraud alert" on their files that alerts creditors to take additional steps to verify their identity prior to granting credit in their names. Please note, however, that because it tells creditors to follow certain procedures to protect the individual's credit, it may also delay the ability to obtain credit while the agency verifies the individual's identity. As soon as one credit bureau confirms an individual's fraud alert, the others are notified to place fraud alerts on that individual's file. Any individual wishing to place a fraud alert, or who has questions regarding their credit report, can contact any one of the following agencies: Equifax, P.O. Box 105069, Atlanta, GA 30348-5069, 800-525-6285, www.equifax.com; Experian, P.O. Box 2002, Allen, TX 75013, 888-397-3742, www.experian.com; or TransUnion, P.O. Box 2000, Chester, PA 19022-2000, 800-680-7289, www.transunion.com. Information regarding security freezes may also be obtained from these sources.

The Federal Trade Commission (FTC) also encourages those who discover that their information has been misused to file a complaint with them. To file a complaint with the FTC, or to obtain additional information on identity theft and the steps that can be taken to avoid identity theft, the FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, or at www.ftc.gov/idtheft, or (877) ID-THEFT (877-438-4338); TTY: (866) 653-4261. This notice has not been delayed because of law enforcement; however, instances of known or suspected identity theft should be reported to law enforcement, the Attorney General in the individual's state of residence, and the FTC. State Attorneys General may also have advice on preventing identity theft. Patients can also learn more about placing a fraud alert or security freeze on their credit files by contacting the FTC or their state's Attorney General. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For

Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us. For Kentucky residents, the Attorney General can be contacted at 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601-3449, 502-696-5389, www.ag.ky.gov.

Toll-free hotline

To better assist those who may potentially have been affected, Medical Informatics Engineering has established a confidential, toll-free hotline to answer questions. This hotline is available Monday through Friday, 9:00 a.m. to 9:00 p.m. E.T., and can be reached at (866) 328-1987. Updates will be posted to this website.

We take the security of health information very seriously and understand that such incidents cause real concern. We apologize sincerely and thank our customers for their continued loyalty and patience as we work through this challenge.

Massachusetts residents can click here for additional information.

NoMoreClipboard Notice to Individuals of a Data Security Compromise

Fort Wayne, Indiana, June 10, 2015 On behalf of itself and its affected clients, NoMoreClipboard is writing to provide notice of a data security compromise that has affected the security of some protected health information relating to certain clients and individuals who have used a NoMoreClipboard personal health record or patient portal.

On May 26, 2015, we discovered suspicious activity in one of our servers. We immediately began an investigation to identify and remediate any identified security vulnerability. Our first priority is to safeguard the security of patient health information, and we are working with a team of third-party experts to investigate the attack and enhance data security and protection. This investigation is ongoing. On May 26, 2015, we also reported this incident to law enforcement including the FBI Cyber Squad. Law enforcement is actively investigating this matter, and we are cooperating fully with law enforcement's investigation. The investigation indicates this is a sophisticated cyber attack.

Information Compromised

While investigations into this incident are ongoing, we determined that the security of some protected health information contained in NoMoreClipboard accounts has been affected. The affected data relating to individuals who used a NoMoreClipboard portal/personal health record may include an individuals' name, home address, username, hashed password, security question and answer, email address, date of birth, health information, and Social Security number. No financial or credit card information has been compromised, as we do not collect or store this information. Our forensic investigation indicates the unauthorized access to our network began on May 7, 2015. At this time we are working to quantify the number of patients affected by this incident.

We strongly encourage all NoMoreClipboard users to change their passwords. We also strongly encourage everyone to use different passwords for each of their various accounts. Do not use the same password twice. The next time a NoMoreClipboard user logs in, we will prompt a password change. As part of the password change process, users will be sent a 5 digit PIN code to either a cell phone, via an automated phone call, or to an email address already associated with the NoMoreClipboard account. Users will have to enter this 5 digit code to reset their password. We are also emailing NoMoreClipboard users to encourage this password change.

Notification

On June 2, 2015, we began contacting and mailing notice letters disclosing this incident to affected NoMoreClipboard clients.

Affected individuals for whom we have a valid postal address will also be notified of this incident through U.S. mail. We will also be disclosing this incident to certain state and federal regulators.

Identity protection services

As the investigations continue, and out of an abundance of caution, we are offering credit monitoring and identity protection services to affected individuals, free of charge, for the next 24 months.

We have established a toll-free call center to answer questions relating to this data security event and the support and services being provided.

Fraud prevention tips

We suggest that affected individuals remain vigilant and seek to protect against possible identity theft or other financial loss by reviewing account statements, notifying their credit card companies, healthcare providers, and insurers of the data compromise, and monitoring their credit reports. Affected individuals may also review Explanation of Benefits statements for irregularities. If an individual does not receive regular Explanation of Benefits statements, he or she can contact his or her health plan and request them to send such statements following the provision of services.

Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, visit www.annualcreditreport.com or call, toll-free, (877) 322-8228.

At no charge, potentially affected individuals can also have these credit bureaus place a "fraud alert" on their files that alerts creditors to take additional steps to verify their identity prior to granting credit in their names. Please note, however, that because it tells creditors to follow certain procedures to protect the individual's credit, it may also delay the ability to obtain credit while the agency verifies the individual's identity. As soon as one credit bureau confirms an individual's fraud alert, the others are notified to place fraud alerts on that individual's file. Any individual wishing to place a fraud alert, or who has questions regarding their credit report, can contact any one of the following agencies: Equifax, P.O. Box 105069, Atlanta, GA 30348-5069, 800-525-6285, www.equifax.com; Experian, P.O. Box 2002, Allen, TX 75013, 888-397-3742, www.experian.com; or TransUnion, P.O. Box 2000, Chester, PA 19022-2000, 800-680-7289, www.transunion.com. Information regarding security freezes may also be obtained from these sources.

The Federal Trade Commission (FTC) also encourages those who discover that their information has been misused to file a complaint with them. To file a complaint with the FTC, or to obtain additional information on identity theft and the steps that can be taken to avoid identity theft, the FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, or at www.ftc.gov/idtheft, or (877) ID-THEFT (877-438-4338); TTY: (866) 653-4261. This notice has not been delayed because of law enforcement; however, instances of known or suspected identity theft should be reported to law enforcement, the Attorney General in the individual's state of residence, and the FTC. State Attorneys General may also have advice on preventing identity theft. Individuals can also learn more about placing a fraud alert or security freeze on their credit files by contacting the FTC or their state's Attorney General. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor,

Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us. For Kentucky residents, the Attorney General can be contacted at 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601-3449, 502-696-5389, www.ag.ky.gov.

Toll-free hotline

To better assist those who may potentially have been affected, we have established a confidential, toll-free hotline to answer questions. This hotline is available Monday through Friday, 9:00 a.m. to 9:00 p.m. E.T., and can be reached at (866) 328-1987. Updated will be posted to this website.

We take the security of health information very seriously and understand that such incidents cause real concern. We apologize sincerely and thank our customers for their continued loyalty and patience as we work through this challenge.

Massachusetts residents can click here for additional information.

EXHIBIT C

PRESS CONTACT: MELANIE THOMAS
mthomas@informtheagency.com
202-390-7887

STATEMENT REGARDING MEDICAL INFORMATICS ENGINEERING'S RECENT CYBER ATTACK

A Message from Eric Jones
Co-Founder & COO, Medical Informatics Engineering
June 10, 2015

A sophisticated cyber attack has compromised some of the protected health information contained on our Medical Informatics Engineering and NoMoreClipboard networks. As soon as we detected suspicious activity on May 26, we launched an internal investigation, retained independent third-party forensics experts, and alerted law enforcement, including the FBI Cyber Squad. Our initial investigation indicates that the unauthorized access to our network began on May 7, 2015.

Our first priority is to safeguard the security of patient health information. We are working with a team of IT security experts to investigate the attack and enhance data security and protection.

Affected data includes names, addresses, dates of birth, social security numbers and other protected health information. No financial or credit card information has been compromised, as we do not collect or store that information.

We are working diligently to determine how many patients were affected by this incident, and we have notified affected healthcare provider clients and business associates. Individuals will be notified by letter if their information was compromised.

We are offering credit monitoring and identity protection services to affected individuals, free of charge, for the next 24 months. We have also established a toll-free call center to answer questions about this attack and the support and services being provided.

We take the security of health information very seriously and understand that such incidents cause real concern. We apologize sincerely and thank our customers for their continued loyalty and patience as we work through this challenge.

For more information, please contact the toll-free call center at 866-328-1987.

Medical Informatics Engineering notifies
Patients of a Data Security Compromise

Fort Wayne, Indiana, June 10, 2015 – On behalf of itself and its affected clients, Medical Informatics Engineering is writing to provide notice of a data security compromise that has affected the security of some protected health information relating to certain patients affiliated with certain Medical Informatics Engineering clients. *We emphasize that the patients of only certain clients of Medical Informatics Engineering were affected by this compromise and those clients have all been notified.* Clients include: Concentra, Fort Wayne Neurological Center, Franciscan St. Francis Health Indianapolis, Gynecology Center, Inc. Fort Wayne, and Rochester Medical Group.

On May 26, 2015, Medical Informatics Engineering discovered suspicious activity relating to one of its servers. Medical Informatics Engineering immediately began an investigation to identify and remediate any identified security vulnerability. Medical Informatics Engineering's team, including independent third-party forensics experts, has been working continuously to investigate the attack and enhance data security and protection. On May 26, 2015, Medical Informatics Engineering also reported this incident to law enforcement including the FBI Cyber Squad. Law enforcement is actively investigating this matter, and Medical Informatics Engineering is cooperating with law enforcement's investigation. Medical Informatics Engineering's forensic investigation indicates the unauthorized access to our network began on May 7, 2015. The investigation indicates this is a sophisticated cyber attack.

Compromised information

While investigations into this incident are ongoing, Medical Informatics Engineering determined the security of some protected health information contained on Medical Informatics Engineering's network has been affected. The protected health information affected by this incident relates to patients affiliated with certain Medical Informatics Engineering clients identified above and may include the patient's name, mailing address, email address, date of birth, and for some patients a social security number, lab results, dictated reports, and medical conditions. No financial or credit card information has been compromised, as we do not collect or store this information.

Medical Informatics Engineering also determined that this cyber attack compromised protected health information for its NoMoreClipboard subsidiary. Separate notice is being issued for affected clients and patients associated with NoMoreClipboard.

Notification

On June 2, 2015, Medical Informatics Engineering began contacting and mailing notice letters disclosing this incident to affected Medical Informatics Engineering clients.

Affected patients for whom Medical Informatics Engineering has a valid postal address will be notified of this incident through U.S. mail. The same information contained in the notice letter will also be available at the Medical Informatics Engineering website – www.mieweb.com. Medical Informatics Engineering will also be disclosing this incident to certain state and federal regulators.

Identity protection services

As the investigations continue, and out of an abundance of caution, Medical Informatics Engineering is offering credit monitoring and identity protection services to affected patients, free of charge, for the next 24 months.

Medical Informatics Engineering has established a toll-free call center to answer questions relating to this data security event and the support and services being provided.

Fraud prevention tips

Medical Informatics Engineering suggests that affected patients remain vigilant and seek to protect against possible identity theft or other financial loss by reviewing account statements, notifying their credit card companies, healthcare providers, and insurers of the data compromise, and monitoring their credit reports. Affected patients may also review Explanation of Benefits statements for irregularities. If an individual does not receive regular Explanation of Benefits statements, he or she can contact his or her health plan and request them to send such statements following the provision of services.

Under U.S. law, patients are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, visit www.annualcreditreport.com or call, toll-free, (877) 322-8228.

At no charge, potentially affected patients can also have these credit bureaus place a "fraud alert" on their files that alerts creditors to take additional steps to verify their identity prior to granting credit in their names. Please note, however, that because it tells creditors to follow certain procedures to protect the individual's credit, it may also delay the ability to obtain credit while the agency verifies the individual's identity. As soon as one credit bureau confirms an individual's fraud alert, the others are notified to place fraud alerts on that individual's file. Any individual wishing to place a fraud alert, or who has questions regarding their credit report, can contact any one of the following agencies: Equifax, P.O. Box 105069, Atlanta, GA 30348-5069, 800-525-6285, www.equifax.com; Experian, P.O. Box 2002, Allen, TX 75013, 888-397-3742, www.experian.com; or TransUnion, P.O. Box 2000, Chester, PA 19022-2000, 800-680-7289, www.transunion.com. Information regarding security freezes may also be obtained from these sources.

The Federal Trade Commission (FTC) also encourages those who discover that their information has been misused to file a complaint with them. To file a complaint with the FTC, or to obtain additional information on identity theft and the steps that can be taken to avoid identity theft, the FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, or at www.ftc.gov/idtheft, or (877) ID-THEFT (877-438-4338); TTY: (866) 653-4261. This notice has not been delayed because of law enforcement; however, instances of known or suspected identity theft should be reported to law enforcement, the Attorney General in the individual's state of residence, and the FTC. State Attorneys General may also have advice on preventing identity theft. Patients can also learn more about placing a fraud alert or security freeze on their credit files by contacting the FTC or their state's Attorney General. For North Carolina residents, the Attorney General can be contacted at

9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us. For Kentucky residents, the Attorney General can be contacted at 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601-3449, 502-696-5389, www.ag.ky.gov.

Toll-free hotline

To better assist those who may potentially have been affected, Medical Informatics Engineering has established a confidential, toll-free hotline to answer questions. This hotline is available Monday through Friday, 9:00 a.m. to 9:00 p.m. E.T., and can be reached at (866) 328-1987. Affected patients can also visit www.mieweb.com for additional information and updates.

We take the security of health information very seriously and understand that such incidents cause real concern. We apologize sincerely and thank our customers for their continued loyalty and patience as we work through this challenge.

NoMoreClipboard Notice to
Individuals of a Data Security Compromise

Fort Wayne, Indiana, June 10, 2015 On behalf of itself and its affected clients, NoMoreClipboard is writing to provide notice of a data security compromise that has affected the security of some protected health information relating to certain clients and individuals who have used a NoMoreClipboard personal health record or patient portal.

On May 26, 2015, we discovered suspicious activity in one of our servers. We immediately began an investigation to identify and remediate any identified security vulnerability. Our first priority is to safeguard the security of patient health information, and we are working with a team of third-party experts to investigate the attack and enhance data security and protection. This investigation is ongoing. On May 26, 2015, we also reported this incident to law enforcement including the FBI Cyber Squad. Law enforcement is actively investigating this matter, and we are cooperating fully with law enforcement's investigation. The investigation indicates this is a sophisticated cyber attack.

Information compromised

While investigations into this incident are ongoing, we determined that the security of some protected health information contained in NoMoreClipboard accounts has been affected. The affected data relating to individuals who used a NoMoreClipboard portal/personal health record may include an individuals' name, home address, username, hashed password, security question and answer, email address, date of birth, health information, and Social Security number. No financial or credit card information has been compromised, as we do not collect or store this information. Our forensic investigation indicates the unauthorized access to our network began on May 7, 2015. At this time we are working to quantify the number of patients affected by this incident.

We strongly encourage all NoMoreClipboard users to change their passwords. We also strongly encourage everyone to use different passwords for each of their various accounts. Do not use the same password twice. The next time a NoMoreClipboard user logs in, we will prompt a password change. As part of the password change process, users will be sent a 5 digit PIN code to either a cell phone, via an automated phone call, or to an email address already associated with the NoMoreClipboard account. Users will have to enter this 5 digit code to reset their password. We are also emailing NoMoreClipboard users to encourage this password change.

Notification

On June 2, 2015, we began contacting and mailing notice letters disclosing this incident to affected NoMoreClipboard clients.

Affected individuals for whom we have a valid postal address will also be notified of this incident through U.S. mail. The same information contained in the notice letter will also be available at www.NoMoreClipboard.com. We will also be disclosing this incident to certain state and federal regulators.

Identity protection services

As the investigations continue, and out of an abundance of caution, we are offering credit monitoring and identity protection services to affected individuals, free of charge, for the next 24 months.

We have established a toll-free call center to answer questions relating to this data security event and the support and services being provided.

Fraud prevention tips

We suggest that affected individuals remain vigilant and seek to protect against possible identity theft or other financial loss by reviewing account statements, notifying their credit card companies, healthcare providers, and insurers of the data compromise, and monitoring their credit reports. Affected individuals may also review Explanation of Benefits statements for irregularities. If an individual does not receive regular Explanation of Benefits statements, he or she can contact his or her health plan and request them to send such statements following the provision of services.

Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, visit www.annualcreditreport.com or call, toll-free, (877) 322-8228.

At no charge, potentially affected individuals can also have these credit bureaus place a "fraud alert" on their files that alerts creditors to take additional steps to verify their identity prior to granting credit in their names. Please note, however, that because it tells creditors to follow certain procedures to protect the individual's credit, it may also delay the ability to obtain credit while the agency verifies the individual's identity. As soon as one credit bureau confirms an individual's fraud alert, the others are notified to place fraud alerts on that individual's file. Any individual wishing to place a fraud alert, or who has questions regarding their credit report, can contact any one of the following agencies: Equifax, P.O. Box 105069, Atlanta, GA 30348-5069, 800-525-6285, www.equifax.com; Experian, P.O. Box 2002, Allen, TX 75013, 888-397-3742, www.experian.com; or TransUnion, P.O. Box 2000, Chester, PA 19022-2000, 800-680-7289, www.transunion.com. Information regarding security freezes may also be obtained from these sources.

The Federal Trade Commission (FTC) also encourages those who discover that their information has been misused to file a complaint with them. To file a complaint with the FTC, or to obtain additional information on identity theft and the steps that can be taken to avoid identity theft, the FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, or at www.ftc.gov/idtheft, or (877) ID-THEFT (877-438-4338); TTY: (866) 653-4261. This notice has not been delayed because of law enforcement; however, instances of known or suspected identity theft should be reported to law enforcement, the Attorney General in the individual's state of residence, and the FTC. State Attorneys General may also have advice on preventing identity theft. Individuals can also learn more about placing a fraud alert or security freeze on their credit files by contacting the FTC or their state's Attorney General. For North Carolina residents, the Attorney General can be contacted at

9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us. For Kentucky residents, the Attorney General can be contacted at 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601-3449, 502-696-5389, www.ag.ky.gov.

Toll-free hotline

To better assist those who may potentially have been affected, we have established a confidential, toll-free hotline to answer questions. This hotline is available Monday through Friday, 9:00 a.m. to 9:00 p.m. E.T., and can be reached at (866) 328-1987. Affected individuals can also visit www.NoMoreClipboard.com for additional information and updates.

We take the security of health information very seriously and understand that such incidents cause real concern. We apologize sincerely and thank our customers for their continued loyalty and patience as we work through this challenge.

EXHIBIT B

NoMoreClipBoard Affected Covered Entities

Advanced Cardiac Care
Advanced Foot Specialists
All About Childrens Pediatric Partners, PC
Allen County Dept of Health
Allied Physicians, Inc. d/b/a Fort Wayne Neurological Center (including Neurology, Physical Medicine and Neurosurgery)
Altagracia Medical Center
Anderson Family Medicine
Arkansas Otolaryngology, P.A.
Auburn Cardiology Associates
Basedow Family Clinic Inc.
Bastrop Medical Clinic
Batish Family Medicine
Beaver Medical
Boston Podiatry Services PC
Brian Griner M.D.
Brightstarts Pediatrics
Burnsville Medical Center
Capital Rehabilitation
Cardiovascular Consultants of Kansas
Carl Gustafson OD
Carolina Gastroenterology
Carolina Kidney & Hypertension Center
Carolinas Psychiatric Associates
Center for Advanced Spinal Surgery
Chang Neurosurgery & Spine Care
Cheyenne County Hospital
Children's Clinic of Owasso, P.C.
Clara A. Lennox MD
Claude E. Younes M.D., Inc.
CMMC
Coalville Health Center
Cornerstone Medical and Wellness, LLC
Cumberland Heart
David A. Wassil, D.O.
David M Mayer MD
Dr. Alicia Guice
Dr. Anne Hughes
Dr. Buchele
Dr. Clark
Dr. Harvey
Dr. John Labban
Dr. John Suen
Dr. Puleo
Dr. Rajesh Rana
Dr. Rustagi
Dr. Schermerhorn
Dr. Shah

Ear, Nose & Throat Associates, P.C.
East Carolina Medical Associates
Eastern Washington Dermatology Associates
Ellinwood District Hospital
Family Care Chiropractic Center
Family Practice Associates of Macomb
Family Practice of Macomb
Floyd Trillis Jr., M.D.
Fredonia Regional Hospital
Fremont Family Medicine
Generations Primary Care
Grace Community Health Center, Inc.
Grisell Memorial Hospital
Harding Pediatrics LLP
Harlan County Health System
Health Access Program
Heart Institute of Venice
Henderson Minor Outpatient Medicine
Henry County Hospital myhealth portal
Highgate Clinic
Hobart Family Medical Clinic
Howard Stierwalt, M.D.
Howard University Hospital
Hudson Essex Nephrology
Huntington Medical Associates
Huntington Medical Group
Hutchinson Regional Medical Center
Idaho Sports Medicine Institute
In Step Foot & Ankle Specialists
Independence Rehabilitation Inc
Indiana Endocrine Specialists
Indiana Internal Medicine Consultants
Indiana Ohio Heart
Indiana Surgical Specialists
Indiana University
Indiana University Health Center
Indianapolis Gastroenterology and Hepatology
Internal Medicine Associates
IU - Northwest
Jackson Neurolosurgery Clinic
James E. Hunt, MD
Jasmine K. Leong MD
Jewell County Hospital
John Hiestand, M.D.
Jonathan F. Diller, M.D.
Jubilee Community Health
Kardous Primary Care
Keith A. Harvey, M.D.
Kenneth Cesa DPM
Kings Clinic and Urgent Care
Kiowa County Memorial Hospital

Kristin Egan MD
Lakeshore Family Practice
Lane County Hospital
Logan County Hospital
Margaret Mary Health
Masonboro Urgent Care
McDonough Medical Group Psychiatry
Medical Care, Inc.
Medical Center of East Houston
Medicine Lodge Memorial Hospital
MedPartners
MHP Cardiology
Michael Mann, MD, PC
Michelle Barnes Marshall, P.C.
Michiana Gastroenterology, Inc.
Minneola District Hospital
Mora Surgical Clinic
Moundridge Mercy Hospital Inc
myhealthnow
Nancy L. Carteron M.D.
Naples Heart Rhythm Specialists
Nate Delisi DO
Neighborhood Health Clinic
Neosho Memorial Regional Medical Center
Neuro Spine Pain Surgery Center
Norman G. McKoy, M.D. & Ass., P.A.
North Corridor Internal Medicine
Nova Pain Management
Novapex Franklin
Oakland Family Practice
Oakland Medical Group
Ohio Physical Medicine & Rehabilitation Inc.
On Track For Life
Ottawa County Health Center
Pareshchandra C. Patel MD
Parkview Health System, Inc. d/b/a Family Practice Associates of Huntington
Parkview Health System, Inc. d/b/a Fort Wayne Cardiology
Parrott Medical Clinic
Partners In Family Care
Personalized Health Care Of Tucson
Phillips County Hospital
Physical Medicine Consultants
Physicians of North Worchester County
Precision Weight Loss Center
Primary & Alternative Medical Center
Prince George's County Health Department
Rebecca J. Kurth M.D.
Relief Center
Republic County Hospital
Ricardo S. Lemos MD
Richard A. Stone M.D.

Richard Ganz MD
River Primary Care
Rolando P. Oro MD, PA
Ronald Chochinov
Sabetha Community Hospital
Santa Cruz Pulmonary Medical Group
Santone Chiropractic
Sarasota Cardiovascular Group
Sarasota Center for Family Health Wellness
Sarasota Heart Center
Satanta District Hospital
Saul & Cutarelli MD's Inc.
Shaver Medical Clinic, P. A.
Skiatook Osteopathic Clinic Inc.
Sleep Centers of Fort Wayne
Smith County Hospital
Smith Family Chiropractic
Somers Eye Center
South Forsyth Family Medicine & Pediatrics
Southeast Rehabilitation Associates PC
Southgate Radiology
Southwest Internal Medicine & Pain Management
Southwest Orthopaedic Surgery Specialists,PLC
Stafford County Hospital
Stephen Helvie MD
Stephen T. Child MD
Susan A. Kubica MD
Texas Childrens Hospital
The Children's Health Place
The Heart & Vascular Specialists
The Heart and Vascular Center of Sarasota
The Imaging Center
The Johnson Center for Pelvic Health
The Medical Foundation, My Lab Results Portal
Thompson Family Chiropractic
Trego County Hospital
Union Square Dermatology
Volunteers in Medicine
Wells Chiropractic Clinic
Wichita County Health Center
William Klope MD
Wyoming Total Health Record Patient Portal
Yovanni Tineo M.D.
Zack Hall M.D.

Medical Informatics Engineering Affected Covered Entities

RediMed
Allied Physicians, Inc. d/b/a Fort Wayne Neurological Center (including Neurology, Physical Medicine and Neurosurgery)
Concentra
Franciscan St. Francis Health Indianapolis
Gynecology Center, Inc. Fort Wayne
Rochester Medical Group
Fort Wayne Radiology Association, LLC (including d/b/a Nuvena Vein Center and Dexa Diagnostics; Open View MRI, LLC; Breast Diagnostic Center, LLC; P.E.T. Imaging Services, LLC; MRI Center -Fort Wayne Radiology, Inc. f/k/a Advanced Imaging Systems, Inc.).

EXHIBIT C

MEDICAL INFORMATICS ENGINEERING

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<mail id>>
<<first name>> <<last name>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Re: Notice of Data Security Event

Dear <<First Name>> <<Last Name>>,

My name is Eric Jones and I am co-founder and COO of Medical Informatics Engineering. Our companies provide electronic medical record, patient portal and personal health record services to certain healthcare providers and other clients, including:

<<*Healthcare Provider 1>>
<<*Healthcare Provider 2>>
<<*Healthcare Provider 3>>
<<*Healthcare Provider 4>>
<<*Healthcare Provider 5>>
<<*Healthcare Provider 6>>
<<*Healthcare Provider 7>>
<<*Healthcare Provider 8>>
<<*Healthcare Provider 9>>
<<*Healthcare Provider 10>>

On behalf of Medical Informatics Engineering, I am writing to notify you that a data security compromise occurred at Medical Informatics Engineering that has affected the security of some of your personal and protected health information. This letter contains details about the incident and our response, steps you can take to protect your information, and resources we are making available to help you.

What happened? On May 26, 2015, Medical Informatics Engineering discovered suspicious activity relating to one of its servers. We immediately began an investigation to identify and remediate any identified security vulnerability. Our first priority is to safeguard the security of personal and protected health information, and we are working with a team of third-party forensics experts to investigate the attack and enhance data security and protection. On May 26, 2015, we also reported this incident to law enforcement including the FBI Cyber Squad. Law enforcement is actively investigating this matter, and we are cooperating fully with law enforcement's investigation. The investigation indicates this is a sophisticated cyber attack. Our forensic investigation indicates the unauthorized access to our network began on May 7, 2015.

While investigations into this incident are ongoing, we determined the security of some personal and protected health information contained on Medical Informatics Engineering's network has been affected. The affected data includes your:

<<*Data Element>>
<<*Data Element>>
<<*Data Element>>
<<*Data Element>>
<<*Data Element>>
<<*Data Element>>
<<*Data Element>>
<<*Data Element>>

For additional information on this incident, your affected data, the identity of your affected healthcare provider(s) and the information which came from each of them, if more than one provider is identified above, please call (866) 328-1987.

What we are doing? We take the security of your information very seriously, and apologize for the inconvenience this matter has caused you. Our investigation, the investigation of our third-party data forensics experts, and law enforcement's investigation, are all ongoing. We are also continuing to take steps to remediate and enhance the security of our systems. Remedial efforts include removing the capabilities used by the intruder to gain unauthorized access to the affected systems, enhancing and strengthening password rules and storage mechanisms, increased active monitoring of the affected systems, and intelligence exchange with law enforcement. We have also instituted a universal password reset.

To help protect your identity, we have engaged Experian®, the largest credit bureau in the U.S., to offer you a complimentary two year membership to Experian's ProtectMyID® Elite credit monitoring and identity restoration services. Instructions on how to enroll and receive these services are included in the attached Notice of Privacy Safeguards.

What you can do? We encourage you to enroll and receive the complimentary membership to Experian's ProtectMyID® Elite services we are offering to you. We also encourage you to take steps described in the enclosed Notice of Privacy Safeguards on how to protect yourself against identity theft and fraud.

We recognize that you may have questions that are not answered in this letter. We have established a confidential, toll free hotline to assist you with questions regarding the incident, your affected personal and protected health information, this letter or Experian's identity monitoring and protection services. The hotline can be reached at (866) 328-1987, Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time, except for holidays. You may also contact Experian directly at (866) 579-4461 for questions regarding the credit monitoring and identity restoration services. You may also visit www.mieweb.com for more information. Updates regarding this incident, our investigation and steps you may take to protect yourself from identity theft and fraud will be available on www.mieweb.com and through our toll free hotline. Questions regarding this letter and the incident should not be directed to your healthcare provider(s) as they may not be able to answer your questions.

We regret any inconvenience this incident may cause. We remain committed to safeguarding the personal and protected health information in our care and will continue to take proactive steps to enhance security.

Sincerely,

Eric Jones
Co-Founder, COO
Medical Informatics Engineering

NOTICE OF PRIVACY SAFEGUARDS

Experian's ProtectMyID® Elite

We encourage you to activate the fraud detection tools available through ProtectMyID® Elite. This product provides you with superior identity protection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

1. ENSURE **That You Enroll By**: 10/25/2015 (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site to enroll**: www.protectmyid.com/protect
3. PROVIDE Your Activation Code: [code]

If you have questions or need an alternative to enrolling online, please call (866) 579-4461 and provide Engagement number: **PC94878**. A credit card is not required for enrollment.

You are also able to immediately contact Experian regarding any fraud issues, and have access to the following features once you initiate ProtectMyID:

- **Experian credit report**: See what information is associated with your credit file.
- **Active Surveillance Alerts**: Monitors the Experian file for indicators of fraud.
- **Internet Scan**: Alerts you if your information is found on sites containing compromised data.
- **Address Change Alerts**: Alerts you of changes to your mailing address
- **Fraud Resolution**: Identity Theft Resolution agents are immediately available to help you address credit and non-credit related fraud.
- **ExtendCARE**: You receive the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance**[1]: Provides coverage for certain costs and unauthorized electronic fund transfers.
- **Lost Wallet Protection**: Get help replacing credit, debit, and medical insurance cards.

You may integrate your ProtectMyID membership with the BillGuard app for FREE and receive:

- **Card Fraud Monitoring**: Alerts you when your credit/debit cards are used.
- **Card Concierge**: Resolve billing inquiries and disputes with merchants

If you are a victim of fraud, simply call Experian at (866) 579-4461 by 10/25/2015 and a dedicated Identity Theft Resolution agent will help you restore your identity. Please provide engagement number **PC94878** as proof of eligibility. If you have any questions about ProtectMyID® Elite, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at (866) 579-4461. For additional information on BillGuard you may visit www.protectmyid.com/billguard.

Additional Steps You Can Take to Protect Yourself

In addition to enrolling in Experian's ProtectMyID® Elite, we encourage you to remain vigilant and seek to protect against possible identity theft or other financial loss by regularly reviewing your financial account statements for charges you did not make. We also encourage you to notify your credit card companies, health care providers, and heathcare insurers of this data security incident. You may also review explanation of benefits statement(s) that you receive from your healthcare provider or health plan. If you see any service that you believe you did not receive, you should contact your health care provider or health plan at the telephone number listed on the explanation of benefits statement(s). If you do not receive regular explanation of benefits statement(s), contact your healthcare provider or health plan and ask that they send you a copy after each visit you make to your health care provider.

We also suggest that you carefully review your credit reports. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, visit www.annualcreditreport.com or call, toll-free, (877) 322-8228.

[1]Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Please note, however, that because it tells creditors to follow certain procedures to protect your credit, it may also delay the ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. If you wish to place a fraud alert, or you have questions regarding your credit report, you can contact any one of the following agencies: **Equifax**, Consumer Fraud Division, P.O. Box 740256, Atlanta, GA 30374, (800) 525-6285, www.equifax.com; **Experian**, Consumer Fraud Assistance, P.O. Box 9556, Allen, TX 75013, (888) 397-3742, www.experian.com; **TransUnion**, Consumer Relations & Fraud Victim Assistance, 1561 E. Orangethorpe Avenue, Fullerton, CA 92831, (800) 372-8391, www.transunion.com. Information regarding security freezes may also be obtained from these sources.

The Federal Trade Commission (FTC) encourages those who discover that their information has been misused to file a complaint with them. To file a complaint with the FTC, or to obtain additional information on identity theft and the steps that can be taken to avoid identity theft, the FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, www.ftc.gov/idtheft, (877) ID-THEFT (877-438-4338); TTY: (866) 653-4261. This notice has not been delayed because of law enforcement; however, instances of known or suspected identity theft should be reported to local law enforcement, your state Attorney General, and the FTC. Your state Attorneys General may also have advice on preventing identity theft. You can also learn more about placing a fraud alert or security freeze on their credit files by contacting the FTC or your state Attorney General. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us. For Kentucky residents, the Attorney General can be contacted at 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601-3449, 502-696-5389, www.ag.ky.gov. For Indiana residents, the Attorney General can be contacted at 302 W. Washington Street, Indianapolis, Indiana 46204, (317) 232-6201, www.in.gov.

Security Freeze

Under MA and WV law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Under MA and WV law, you may place a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without your written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services.

If you have been a victim of identity theft, and provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 in MA and $5.30 in WV each to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving a request to place a security freeze on a credit file report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to remove the security freeze.

MEDICAL INFORMATICS ENGINEERING

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<mail id>>
<<first name>> <<last name>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Re: Notice of Data Security Event

Dear <<first name>> <<last name>>,

My name is Eric Jones and I am co-founder and COO of Medical Informatics Engineering. Our companies provide electronic medical record, patient portal and personal health record services to certain healthcare providers and other clients, including:

<<*Healthcare Provider 1>>
<<*Healthcare Provider 2>>
<<*Healthcare Provider 3>>
<<*Healthcare Provider 4>>
<<*Healthcare Provider 5>>
<<*Healthcare Provider 6>>
<<*Healthcare Provider 7>>
<<*Healthcare Provider 8>>
<<*Healthcare Provider 9>>
<<*Healthcare Provider 10>>

On behalf of Medical Informatics Engineering, I am writing to notify you that a data security compromise occurred at Medical Informatics Engineering that has affected the security of some of your personal and protected health information. This letter contains details about the incident and our response, steps you can take to protect your information, and resources we are making available to help you.

What happened? On May 26, 2015, Medical Informatics Engineering discovered suspicious activity relating to one of its servers. We immediately began an investigation to identify and remediate any identified security vulnerability. Our first priority is to safeguard the security of personal and protected health information, and we are working with a team of third-party forensics experts to investigate the attack and enhance data security and protection. On May 26, 2015, we also reported this incident to law enforcement including the FBI Cyber Squad. Law enforcement is actively investigating this matter, and we are cooperating fully with law enforcement's investigation. The investigation indicates this is a sophisticated cyber attack. Our forensic investigation indicates the unauthorized access to our network began on May 7, 2015.

While investigations into this incident are ongoing, we determined the security of some personal and protected health information contained on Medical Informatics Engineering's network has been affected. The affected data includes your:

<<*Data Element>>
<<*Data Element>>
<<*Data Element>>
<<*Data Element>>
<<*Data Element>>
<<*Data Element>>
<<*Data Element>>
<<*Data Element>>

Other data that may be affected (if not otherwise identified above) includes your: Social Security number, date of birth, address, account number, diagnosis, disability code, health insurance policy information, and health information.

For additional information on this incident, your affected data, the identity of your affected healthcare provider(s) and the information which came from each of them, if more than one provider is identified above, please call (866) 328-1987.

What we are doing? We take the security of your information very seriously, and apologize for the inconvenience this matter has caused you. Our investigation, the investigation of our third-party data forensics experts, and law enforcement's investigation, are all ongoing. We are also continuing to take steps to remediate and enhance the security of our systems. Remedial efforts include removing the capabilities used by the intruder to gain unauthorized access to the affected systems, enhancing and strengthening password rules and storage mechanisms, increased active monitoring of the affected systems, and intelligence exchange with law enforcement. We have also instituted a universal password reset.

To help protect your identity, we have engaged Experian®, the largest credit bureau in the U.S., to offer you a complimentary two year membership to Experian's ProtectMyID® Elite credit monitoring and identity restoration services. Instructions on how to enroll and receive these services are included in the attached Notice of Privacy Safeguards.

What you can do? We encourage you to enroll and receive the complimentary membership to Experian's ProtectMyID® Elite services we are offering to you. We also encourage you to take steps described in the enclosed Notice of Privacy Safeguards on how to protect yourself against identity theft and fraud.

We recognize that you may have questions that are not answered in this letter. We have established a confidential, toll free hotline to assist you with questions regarding the incident, your affected personal and protected health information, this letter or Experian's identity monitoring and protection services. The hotline can be reached at (866) 328-1987, Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time, except for holidays. You may also contact Experian directly at (866) 579-4461 for questions regarding the credit monitoring and identity restoration services. You may also visit www.mieweb.com for more information. Updates regarding this incident, our investigation and steps you may take to protect yourself from identity theft and fraud will be available on www.mieweb.com and through our toll free hotline. Questions regarding this letter and the incident should not be directed to your healthcare provider(s) as they may not be able to answer your questions.

We regret any inconvenience this incident may cause. We remain committed to safeguarding the personal and protected health information in our care and will continue to take proactive steps to enhance security.

Sincerely,

Eric Jones
Co-Founder, COO
Medical Informatics Engineering

NOTICE OF PRIVACY SAFEGUARDS

Experian's ProtectMyID® Elite

We encourage you to activate the fraud detection tools available through ProtectMyID® Elite. This product provides you with superior identity protection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

1. ENSURE **That You Enroll By**: 10/25/2015 (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site to enroll**: www.protectmyid.com/protect
3. PROVIDE Your Activation Code: [code]

If you have questions or need an alternative to enrolling online, please call (866) 579-4461 and provide Engagement number: **PC94878**. A credit card is not required for enrollment.

You are also able to immediately contact Experian regarding any fraud issues, and have access to the following features once you initiate ProtectMyID:

- **Experian credit report**: See what information is associated with your credit file.
- **Active Surveillance Alerts**: Monitors the Experian file for indicators of fraud.
- **Internet Scan**: Alerts you if your information is found on sites containing compromised data.
- **Address Change Alerts**: Alerts you of changes to your mailing address
- **Fraud Resolution**: Identity Theft Resolution agents are immediately available to help you address credit and non-credit related fraud.
- **ExtendCARE**: You receive the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance**[1]: Provides coverage for certain costs and unauthorized electronic fund transfers.
- **Lost Wallet Protection**: Get help replacing credit, debit, and medical insurance cards.

You may integrate your ProtectMyID membership with the BillGuard app for FREE and receive:

- **Card Fraud Monitoring**: Alerts you when your credit/debit cards are used.
- **Card Concierge**: Resolve billing inquiries and disputes with merchants

If you are a victim of fraud, simply call Experian at (866) 579-4461 by 10/25/2015 and a dedicated Identity Theft Resolution agent will help you restore your identity. Please provide engagement number **PC94878** as proof of eligibility. If you have any questions about ProtectMyID® Elite, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at (866) 579-4461. For additional information on BillGuard you may visit www.protectmyid.com/billguard.

Additional Steps You Can Take to Protect Yourself

In addition to enrolling in Experian's ProtectMyID® Elite, we encourage you to remain vigilant and seek to protect against possible identity theft or other financial loss by regularly reviewing your financial account statements for charges you did not make. We also encourage you to notify your credit card companies, health care providers, and heathcare insurers of this data security incident. You may also review explanation of benefits statement(s) that you receive from your healthcare provider or health plan. If you see any service that you believe you did not receive, you should contact your health care provider or health plan at the telephone number listed on the explanation of benefits statement(s). If you do not receive regular explanation of benefits statement(s), contact your healthcare provider or health plan and ask that they send you a copy after each visit you make to your health care provider.

We also suggest that you carefully review your credit reports. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, visit www.annualcreditreport.com or call, toll-free, (877) 322-8228.

---

[1]Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Please note, however, that because it tells creditors to follow certain procedures to protect your credit, it may also delay the ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. If you wish to place a fraud alert, or you have questions regarding your credit report, you can contact any one of the following agencies: **Equifax**, Consumer Fraud Division, P.O. Box 740256, Atlanta, GA 30374, (800) 525-6285, www.equifax.com; **Experian**, Consumer Fraud Assistance, P.O. Box 9556, Allen, TX 75013, (888) 397-3742, www.experian.com; **TransUnion**, Consumer Relations & Fraud Victim Assistance, 1561 E. Orangethorpe Avenue, Fullerton, CA 92831, (800) 372-8391, www.transunion.com. Information regarding security freezes may also be obtained from these sources.

The Federal Trade Commission (FTC) encourages those who discover that their information has been misused to file a complaint with them. To file a complaint with the FTC, or to obtain additional information on identity theft and the steps that can be taken to avoid identity theft, the FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, www.ftc.gov/idtheft, (877) ID-THEFT (877-438-4338); TTY: (866) 653-4261. This notice has not been delayed because of law enforcement; however, instances of known or suspected identity theft should be reported to local law enforcement, your state Attorney General, and the FTC. Your state Attorneys General may also have advice on preventing identity theft. You can also learn more about placing a fraud alert or security freeze on their credit files by contacting the FTC or your state Attorney General. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us. For Kentucky residents, the Attorney General can be contacted at 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601-3449, 502-696-5389, www.ag.ky.gov. For Indiana residents, the Attorney General can be contacted at 302 W. Washington Street, Indianapolis, Indiana 46204, (317) 232-6201, www.in.gov.

Security Freeze

Under MA and WV law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Under MA and WV law, you may place a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without your written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services.

If you have been a victim of identity theft, and provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 in MA and $5.30 in WV each to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving a request to place a security freeze on a credit file report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to remove the security freeze.

MEDICAL INFORMATICS ENGINEERING

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<mail id>>
Parent or Guardian of <<minor(s) name(s)>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Re: Notice of Data Security Event

Dear Parent or Guardian,

My name is Eric Jones and I am co-founder and COO of Medical Informatics Engineering. Our companies provide electronic medical record, patient portal, and personal health record services to certain healthcare providers and other clients, including:

<<*Healthcare Provider 1>>
<<*Healthcare Provider 2>>
<<*Healthcare Provider 3>>
<<*Healthcare Provider 4>>
<<*Healthcare Provider 5>>
<<*Healthcare Provider 6>>
<<*Healthcare Provider 7>>
<<*Healthcare Provider 8>>
<<*Healthcare Provider 9>>
<<*Healthcare Provider 10>>

On behalf of Medical Informatics Engineering, I am writing to notify you that a data security compromise occurred at Medical Informatics Engineering that has affected the security of some of your child's/children's personal and protected health information. This letter contains details about the incident and our response, steps you can take to protect your child's/children's information, and resources we are making available to help you and your child/children.

What happened? On May 26, 2015, Medical Informatics Engineering discovered suspicious activity relating to one of its servers. We immediately began an investigation to identify and remediate any identified security vulnerability. Our first priority is to safeguard the security of personal and protected health information, and we are working with a team of third-party forensics experts to investigate the attack and enhance data security and protection. On May 26, 2015, we also reported this incident to law enforcement, including the FBI Cyber Squad. This notice has not been delayed at the request of law enforcement. However, law enforcement is actively investigating this matter, and we are cooperating fully with law enforcement's investigation. The investigation indicates this is a sophisticated cyber attack. Our forensic investigation indicates the unauthorized access to our network occurred on May 7, 2015.

While investigations into this incident are ongoing, we determined that the security of some personal and protected health information contained on Medical Informatics Engineering's network has been affected. The affected information includes your child/children's:

<<*Data Element>>	<<*Data Element>>
<<*Data Element>>	<<*Data Element>>
<<*Data Element>>	<<*Data Element>>
<<*Data Element>>	<<*Data Element>>

For additional information on this incident, your child's/children's affected data, the identity of your child's/children's affected healthcare provider(s) and the information which came from each of them, if more than one provider is identified above, please call (866) 328-1987.

What we are doing? We take the security of your child's/children's information very seriously, and apologize for the inconvenience this matter has caused you. Our investigation, the investigation of our third-party data forensics experts, and law enforcement's investigation, are all ongoing. We are also continuing to take steps to remediate and enhance the security of our systems. Remedial efforts include removing the capabilities used by the intruder to gain unauthorized access to the affected systems, enhancing and strengthening password rules and storage mechanisms, increased active monitoring of the affected systems, and intelligence exchange with law enforcement. We have also instituted a universal password reset.

To help protect your child's/children's identity we have engaged Experian®, the largest credit bureau in the U.S. We are providing you, the parent or guardian, with a complimentary two year membership to Family Secure®. Information on Family Secure® is included in the attached Notice of Privacy Safeguards.

What you can do? We encourage you to enroll and receive the complimentary membership to Experian's Family Secure® services we are offering to your child/children. We also encourage you to take the steps described in the enclosed Notice of Privacy Safeguards on how to protect your child/children against identity theft and fraud.

We recognize that you may have questions that are not answered in this letter. We have established a confidential, toll free hotline to assist you with questions regarding the incident, your child's/children's affected personal and protected health information, this letter or Experian's Family Secure® services. The hotline can be reached at (866) 328-1987, Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time, except for holidays. You may also contact Experian directly at (866) 579-4461 for additional questions regarding the Family Secure® membership. You may also visit www.mieweb.com for additional information. Updates regarding this incident, our investigation and steps you may take to protect your child/children from identity theft and fraud will be available on www.mieweb.com and through our toll free hotline. Questions regarding this letter and the incident should not be directed to your child's/children's health care provider(s) as they may not be able to answer your questions.

We regret any inconvenience this incident may cause. We remain committed to safeguarding the personal and protected health information in our care and will continue to take proactive steps to enhance security.

Sincerely,

Eric Jones
Co-Founder, COO
Medical Informatics Engineering

NOTICE OF PRIVACY SAFEGUARDS

Experian's Family Secure

To receive the complimentary Family Secure membership please call (866) 579-4461 and provide engagement number: **PC94878**. The enrollment deadline is 10/25/2015. Please note that if there are more than one child affected by this data security incident residing in your household, you may enroll all affected minors under the Family Secure same membership. A credit card is not required for enrollment.

Once your Family Secure membership is activated, you, the parent or legal guardian, of the affected minor will receive the following features:

- Daily monitoring of your Experian credit report with email notification of key changes, as well as monthly "no-hit" reports
- 24/7 credit report access: Unlimited, on-demand Experian reports and scores
- Experian credit score illustrator to show monthly score trending and analysis

Children will receive the following features:

- Monthly monitoring to determine whether the enrolled minor in your household has an Experian credit report
- Alerts of key changes to the affected minor's Experian credit report

All Members:

- Identity Theft Resolution assistance: Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies
- $2,000,000 Product Guarantee[1]

Additional Steps You Can Take to Protect Yourself

In addition to enrolling in Experian's Family Secure, we encourage you to remain vigilant and seek to protect against possible identity theft or other financial loss by regularly reviewing your child's/children's financial account statements for any suspicious charges. We also encourage you to notify your child's/children's health care providers and health care insurers of this data security incident.

Under U.S. law, individuals with credit files are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, you may visit www.annualcreditreport.com or call, toll-free, (877) 322-8228. Minors do not have credit files; however, if you order your own credit report, when you receive your credit reports, you should review them carefully. Look for accounts you did not open as well as inquiries from creditors that you did not initiate. Also, you should look for personal information that is not accurate, such as home address or Social Security Number. If you see anything on the report that you do not understand, call the credit reporting agency at the telephone number on the report. If you find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. You should ask for a copy of the police report, as you may need to give copies of the police report to creditors to clear your records. Even if you do not find any signs of fraud on your reports, we recommend that you check your credit reports periodically.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Please note, however, that because it tells creditors to follow certain procedures to protect your credit, it may also delay the ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. If you wish to place a fraud alert, or you have questions regarding your credit report, you can contact any one of the following agencies: **Equifax**, Consumer Fraud Division, P.O. Box 740256, Atlanta, GA 30374, (800) 525-6285, www.equifax.com; **Experian**, Consumer Fraud Assistance, P.O. Box 9556, Allen, TX 75013, (888) 397-3742, www.experian.com; **TransUnion**, Consumer Relations & Fraud Victim Assistance, 1561 E. Orangethorpe Avenue, Fullerton, CA 92831, (800) 372-8391, www.transunion.com. Information regarding security freezes may also be obtained from these sources. Information regarding security freezes may also be obtained from these sources.

[1]The Family Secure Product Guarantee is not available for Individuals who are residents of the state of New York.

The Federal Trade Commission (FTC) encourages those who discover that their information has been misused to file a complaint with them. To file a complaint with the FTC, or to obtain additional information on identity theft and the steps that can be taken to avoid identity theft, the FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, www.ftc.gov/idtheft, (877) ID-THEFT (877-438-4338); TTY: (866) 653-4261. This notice has not been delayed because of law enforcement; however, instances of known or suspected identity theft should be reported to local law enforcement, your state Attorney General, and the FTC. Your state Attorneys General may also have advice on preventing identity theft. You can also learn more about placing a fraud alert or security freeze on your credit files by contacting the FTC or your state Attorney General. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us. For Kentucky residents, the Attorney General can be contacted at 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601-3449, 502-696-5389, www.ag.ky.gov. For Indiana residents, the Attorney General can be contacted at 302 W. Washington Street, Indianapolis, Indiana 46204, (317) 232-6201, www.in.gov.

We also recommend that you regularly review the explanation of benefits statement(s) that you receive, on behalf of your child/children, from his or her health care provider or health plan. If you see any service that you believe your child/children did not receive, you should contact the health care provider or health plan at the telephone number listed on the explanation of benefits statements. If you do not receive regular explanation of benefits statements, contact your child's/children's health care provider or health plan and ask that they send you a copy after each visit you make to your child's/children's health care provider.

Security Freeze

Under MA and WV law, your child has the right to obtain any police report filed in regard to this incident. If your child/children is/are the victim of identity theft, he or she also has the right to file a police report and obtain a copy of it. Under MA and WV law, individuals with credit files may place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without your written authorization. However, please be advised that placing a security freeze on a credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services.

Victims of identity theft that provide the credit reporting agency with a valid police report, cannot be charged to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 in MA and $5.30 in WV each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving a request to place a security freeze on a credit file report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security fre

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to remove the security freeze.

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<mail id>>
Parent or Guardian of <<minor(s) name(s)>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Re: Notice of Data Security Event

Dear Parent or Guardian,

My name is Eric Jones and I am co-founder and COO of Medical Informatics Engineering. Our companies provide electronic medical record, patient portal, and personal health record services to certain healthcare providers and other clients, including:

<<*Healthcare Provider 1>>
<<*Healthcare Provider 2>>
<<*Healthcare Provider 3>>
<<*Healthcare Provider 4>>
<<*Healthcare Provider 5>>
<<*Healthcare Provider 6>>
<<*Healthcare Provider 7>>
<<*Healthcare Provider 8>>
<<*Healthcare Provider 9>>
<<*Healthcare Provider 10>>

On behalf of Medical Informatics Engineering, I am writing to notify you that a data security compromise occurred at Medical Informatics Engineering that has affected the security of some of your child's/children's personal and protected health information. This letter contains details about the incident and our response, steps you can take to protect your child's/children's information, and resources we are making available to help you and your child/children.

What happened? On May 26, 2015, Medical Informatics Engineering discovered suspicious activity relating to one of its servers. We immediately began an investigation to identify and remediate any identified security vulnerability. Our first priority is to safeguard the security of personal and protected health information, and we are working with a team of third-party forensics experts to investigate the attack and enhance data security and protection. On May 26, 2015, we also reported this incident to law enforcement, including the FBI Cyber Squad. This notice has not been delayed at the request of law enforcement. However, law enforcement is actively investigating this matter, and we are cooperating fully with law enforcement's investigation. The investigation indicates this is a sophisticated cyber attack. Our forensic investigation indicates the unauthorized access to our network occurred on May 7, 2015.

While investigations into this incident are ongoing, we determined that the security of some personal and protected health information contained on Medical Informatics Engineering's network has been affected. The affected information includes your child/children's:

<<*Data Element>>
<<*Data Element>>
<<*Data Element>>
<<*Data Element>>
<<*Data Element>>
<<*Data Element>>
<<*Data Element>>
<<*Data Element>>

Other data that may be affected (if not otherwise identified above) includes your child's/children's: Social Security number, date of birth, address, account number, diagnosis, disability code, health insurance policy information and health information.

For additional information on this incident, your child's/children's affected data, the identity of your child's/children's affected healthcare provider(s) and the information which came from each of them, if more than one provider is identified above, please call (866) 328-1987.

What we are doing? We take the security of your child's/children's information very seriously, and apologize for the inconvenience this matter has caused you. Our investigation, the investigation of our third-party data forensics experts, and law enforcement's investigation, are all ongoing. We are also continuing to take steps to remediate and enhance the security of our systems. Remedial efforts include removing the capabilities used by the intruder to gain unauthorized access to the affected systems, enhancing and strengthening password rules and storage mechanisms, increased active monitoring of the affected systems, and intelligence exchange with law enforcement. We have also instituted a universal password reset.

To help protect your child's/children's identity we have engaged Experian®, the largest credit bureau in the U.S. We are providing you, the parent or guardian, with a complimentary two year membership to Family Secure®. Information on Family Secure® is included in the attached Notice of Privacy Safeguards.

What you can do? We encourage you to enroll and receive the complimentary membership to Experian's Family Secure® services we are offering to your child/children. We also encourage you to take the steps described in the enclosed Notice of Privacy Safeguards on how to protect your child/children against identity theft and fraud.

We recognize that you may have questions that are not answered in this letter. We have established a confidential, toll free hotline to assist you with questions regarding the incident, your child's/children's affected personal and protected health information, this letter or Experian's Family Secure® services. The hotline can be reached at (866) 328-1987, Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time, except for holidays. You may also contact Experian directly at (866) 579-4461 for additional questions regarding the Family Secure® membership. You may also visit www.mieweb.com for additional information. Updates regarding this incident, our investigation and steps you may take to protect your child/children from identity theft and fraud will be available on www.mieweb.com and through our toll free hotline. Questions regarding this letter and the incident should not be directed to your child's/children's health care provider(s) as they may not be able to answer your questions.

We regret any inconvenience this incident may cause. We remain committed to safeguarding the personal and protected health information in our care and will continue to take proactive steps to enhance security.

Sincerely,

Eric Jones
Co-Founder, COO
Medical Informatics Engineering

NOTICE OF PRIVACY SAFEGUARDS

Experian's Family Secure
To receive the complimentary Family Secure membership please call (866) 579-4461 and provide engagement number: **PC94878**. The enrollment deadline is 10/25/2015. Please note that if there are more than one child affected by this data security incident residing in your household, you may enroll all affected minors under the Family Secure same membership. A credit card is not required for enrollment.

Once your Family Secure membership is activated, you, the parent or legal guardian, of the affected minor will receive the following features:

- Daily monitoring of your Experian credit report with email notification of key changes, as well as monthly "no-hit" reports
- 24/7 credit report access: Unlimited, on-demand Experian reports and scores
- Experian credit score illustrator to show monthly score trending and analysis

Children will receive the following features:

- Monthly monitoring to determine whether the enrolled minor in your household has an Experian credit report
- Alerts of key changes to the affected minor's Experian credit report

All Members:

- Identity Theft Resolution assistance: Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies
- $2,000,000 Product Guarantee[1]

Additional Steps You Can Take to Protect Yourself
In addition to enrolling in Experian's Family Secure, we encourage you to remain vigilant and seek to protect against possible identity theft or other financial loss by regularly reviewing your child's/children's financial account statements for any suspicious charges. We also encourage you to notify your child's/children's health care providers and health care insurers of this data security incident.

Under U.S. law, individuals with credit files are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, you may visit www.annualcreditreport.com or call, toll-free, (877) 322-8228. Minors do not have credit files; however, if you order your own credit report, when you receive your credit reports, you should review them carefully. Look for accounts you did not open as well as inquiries from creditors that you did not initiate. Also, you should look for personal information that is not accurate, such as home address or Social Security Number. If you see anything on the report that you do not understand, call the credit reporting agency at the telephone number on the report. If you find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. You should ask for a copy of the police report, as you may need to give copies of the police report to creditors to clear your records. Even if you do not find any signs of fraud on your reports, we recommend that you check your credit reports periodically.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Please note, however, that because it tells creditors to follow certain procedures to protect your credit, it may also delay the ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. If you wish to place a fraud alert, or you have questions regarding your credit report, you can contact any one of the following agencies: **Equifax**, Consumer Fraud Division, P.O. Box 740256, Atlanta, GA 30374, (800) 525-6285, www.equifax.com; **Experian**, Consumer Fraud Assistance, P.O. Box 9556, Allen, TX 75013, (888) 397-3742, www.experian.com; **TransUnion**, Consumer Relations & Fraud Victim Assistance, 1561 E. Orangethorpe Avenue, Fullerton, CA 92831, (800) 372-8391, www.transunion.com. Information regarding security freezes may also be obtained from these sources. Information regarding security freezes may also be obtained from these sources.

[1]The Family Secure Product Guarantee is not available for Individuals who are residents of the state of New York.

The Federal Trade Commission (FTC) encourages those who discover that their information has been misused to file a complaint with them. To file a complaint with the FTC, or to obtain additional information on identity theft and the steps that can be taken to avoid identity theft, the FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, www.ftc.gov/idtheft, (877) ID-THEFT (877-438-4338); TTY: (866) 653-4261. This notice has not been delayed because of law enforcement; however, instances of known or suspected identity theft should be reported to local law enforcement, your state Attorney General, and the FTC. Your state Attorneys General may also have advice on preventing identity theft. You can also learn more about placing a fraud alert or security freeze on your credit files by contacting the FTC or your state Attorney General. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us. For Kentucky residents, the Attorney General can be contacted at 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601-3449, 502-696-5389, www.ag.ky.gov. For Indiana residents, the Attorney General can be contacted at 302 W. Washington Street, Indianapolis, Indiana 46204, (317) 232-6201, www.in.gov.

We also recommend that you regularly review the explanation of benefits statement(s) that you receive, on behalf of your child/children, from his or her health care provider or health plan. If you see any service that you believe your child/children did not receive, you should contact the health care provider or health plan at the telephone number listed on the explanation of benefits statements. If you do not receive regular explanation of benefits statements, contact your child's/children's health care provider or health plan and ask that they send you a copy after each visit you make to your child's/children's health care provider.

Security Freeze

Under MA and WV law, your child has the right to obtain any police report filed in regard to this incident. If your child/children is/are the victim of identity theft, he or she also has the right to file a police report and obtain a copy of it. Under MA and WV law, individuals with credit files may place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without your written authorization. However, please be advised that placing a security freeze on a credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services.

Victims of identity theft that provide the credit reporting agency with a valid police report, cannot be charged to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 in MA and $5.30 in WV each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving a request to place a security freeze on a credit file report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to remove the security freeze.

EXHIBIT D

Media Contact: Eric Jones, Medical Informatics Engineering Co-Founder and COO. Please send media inquiries via email to eric@mieweb.com.

Medical Informatics Engineering Updates Notice to Individuals of a Data Security Compromise

Fort Wayne, Indiana, July 24, 2015 On behalf of itself, its NoMoreClipboard subsidiary and its affected clients, Medical Informatics Engineering is writing to provide updated notice of a data security compromise that has affected the security of some personal and protected health information relating to certain clients and individuals who have used a Medical Informatics Engineering electronic health record or a NoMoreClipboard personal health record or patient portal. *We emphasize that the patients of only certain clients of Medical Informatics Engineering and NoMoreClipboard were affected by this compromise and those clients have all been notified.*

On May 26, 2015, we discovered suspicious activity in one of our servers. We immediately began an investigation to identify and remediate any identified security vulnerability. Our first priority was to safeguard the security of personal and protected health information, and we have been working with a team of third-party experts to investigate the attack and enhance data security and protection. This investigation is ongoing. On May 26, 2015, we also reported this incident to law enforcement including the FBI Cyber Squad. Law enforcement is actively investigating this matter, and we are cooperating fully with law enforcement's investigation. The investigation indicates this is a sophisticated cyber attack. Our forensic investigation indicates the unauthorized access to our network began on May 7, 2015. Our monitoring systems helped us detect this unauthorized access, and we were able to shut down the attackers as they attempted to access client data.

We are continuing to take steps to remediate and enhance the security of our systems. Remedial efforts include removing the capabilities used by the intruder to gain unauthorized access to the affected systems, enhancing and strengthening password rules and storage mechanisms, increased active monitoring of the affected systems, and intelligence exchange with law enforcement. We have also instituted a universal password reset.

Information compromised

While investigations into this incident are ongoing, we determined the security of some personal and protected health information contained on Medical Informatics Engineering's network has been affected. The affected data relating to individuals affiliated with affected Medical Informatics Engineering clients may include an individual's name, telephone number, mailing address, username, hashed password, security question and answer, spousal information (name and potentially date of birth), email address, date of birth, Social Security number, lab results, health insurance policy information, diagnosis, disability code, doctor's name, medical conditions, and child's name and birth statistics. The affected data relating to individuals who used a NoMoreClipboard portal/personal health record may include an individuals' name, home address, Social Security number, username, hashed password, spousal information (name and potentially date of birth), security question and answer, email address, date of birth, health information, and health insurance policy information.

Notification

On June 2, 2015, we began contacting and mailing notice letters disclosing this incident to affected NoMoreClipboard and Medical Informatics Engineering clients.

On July 17, 2015, we began mailing notice letters to affected individuals for whom we have a valid postal address through U.S. mail, and we expect those letters to be mailed on or before July 25, 2015. Information contained in the notice letter is available at www.mieweb.com and www.NoMoreClipboard.com. We have also disclosed this incident to certain state and federal regulators and to the consumer reporting agencies.

Identity protection services

As the investigations continue, and out of an abundance of caution, we are offering affected individuals access to two years of credit monitoring and identity protection services at no charge.

Fraud prevention tips

We suggest affected individuals remain vigilant and seek to protect against possible identity theft or other financial loss by regularly reviewing their financial account statements for suspicious activity. We also encourage affected individuals to notify their credit card companies, health care providers, and heath care insurers of this data security incident. Affected individuals may also review explanation of benefits statement(s) that they receive from their healthcare provider or health plan. If an affected individual sees any service that he/she believes he/she did not receive, the individual should contact his/her health care provider or health plan at the telephone number listed on the explanation of benefits statement(s). If an affected individual does not receive regular explanation of benefits statement(s), we suggest he/she contact his/her healthcare provider or health plan and ask that they send a copy after each visit the affected individual makes with his/her health care provider.

We also suggest that affected individuals carefully review their credit reports. Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, visit www.annualcreditreport.com or call, toll-free, (877) 322-8228.

At no charge, individuals can also have these credit bureaus place a "fraud alert" on their file that alerts creditors to take additional steps to verify the his/her identity prior to granting credit in his/her name. Please note, however, that because it tells creditors to follow certain procedures to protect an individual's credit, it may also delay the ability to obtain credit while the agency verifies the individual's identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on an individual's file. If you wish to place a fraud alert, or you have questions regarding your credit report, you can contact any one of the following agencies: **Equifax**, Consumer Fraud Division, P.O. Box 740256, Atlanta, GA 30374, (800) 525-6285, www.equifax.com; **Experian**, Consumer Fraud Assistance, P.O. Box 9556, Allen, TX 75013, (888) 397-3742, www.experian.com; **TransUnion**, Consumer Relations & Fraud Victim Assistance, 1561 E. Orangethorpe Avenue, Fullerton, CA 92831, (800) 372-8391, www.transunion.com. Information regarding security freezes may also be obtained from these sources.

The Federal Trade Commission (FTC) encourages those who discover that their information has been misused to file a complaint with them. To file a complaint with the FTC, or to obtain additional information on identity theft and the steps that can be taken to avoid identity theft, the FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, www.ftc.gov/idtheft, (877) ID-THEFT (877-438-4338); TTY: (866) 653-4261. This notice has not been delayed because of law enforcement; however, instances of known or suspected identity theft should be reported to local law enforcement, your state Attorney General, and the FTC. State Attorneys General may also have advice on preventing identity theft. Individuals can also learn more about placing a fraud alert or security freeze on their credit files by contacting the FTC or state Attorney General. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us. For Kentucky residents, the Attorney General can be contacted at 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601-3449, 502-696-5389, www.ag.ky.gov. For Indiana residents, the Attorney General can be contacted at 302 W. Washington Street, Indianapolis, Indiana 46204, (317) 232-6201, www.in.gov.

Security Freeze

Under MA and WV law, affected individuals have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Under MA and WV law, you may place a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without your written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services.

If you have been a victim of identity theft, and provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 in MA and $5.30 in WV each to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving a request to place a security freeze on a credit file report. The credit bureaus must also send written confirmation to the individual within five (5) business days and provide individual with a unique personal identification number (PIN) or password, or both, that can be used to authorize the removal or lifting of the security freeze. To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to remove the security freeze.

Toll-free hotline

We have established a confidential, toll free hotline to assist affected individuals with questions regarding the incident, their affected personal and protected health information, their affected healthcare provider(s), and the identity monitoring and protection services we are making available. The hotline can be reached at (866) 328-1987, Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time, except for holidays. If you would like to confirm whether you are affected by this incident, you may call our hotline. Updates regarding this incident, our investigation and steps individuals may take to protect themselves from identity theft and fraud will be available on www.nomoreclipboard.com and www.mieweb.com and through our toll free hotline. Questions regarding the incident should not be directed to your healthcare provider(s) as they may not be able to answer your questions.

Affected entities

Physician practices, hospitals, and other organizations work with NoMoreClipboard to offer patient portals and personal health records which enable consumers to access and manage health information online. Individuals who use patient portals or personal health records offered by the following entities may be affected by this cyber attack. Individual notice letters have been sent to affected individuals for whom we have a valid mailing address. Affected organizations include:

Advanced Cardiac Care
Advanced Foot Specialists
All About Childrens Pediatric Partners, PC
Allen County Dept of Health
Allied Physicians, Inc. d/b/a Fort Wayne Neurological Center (including Neurology, Physical Medicine and Neurosurgery)
Altagracia Medical Center
Anderson Family Medicine

Arkansas Otolaryngology, P.A.
Auburn Cardiology Associates
Basedow Family Clinic Inc.
Bastrop Medical Clinic
Batish Family Medicine
Beaver Medical
Boston Podiatry Services PC
Brian Griner M.D.
Brightstarts Pediatrics
Burnsville Medical Center
Capital Rehabilitation
Cardiovascular Consultants of Kansas
Carl Gustafson OD
Carolina Gastroenterology
Carolina Kidney & Hypertension Center
Carolinas Psychiatric Associates
Center for Advanced Spinal Surgery
Chang Neurosurgery & Spine Care
Cheyenne County Hospital
Children's Clinic of Owasso, P.C.
Clara A. Lennox MD
Claude E. Younes M.D., Inc.
CMMC
Coalville Health Center
Cornerstone Medical and Wellness, LLC
Cumberland Heart
David A. Wassil, D.O.
David M Mayer MD
Dr. Alicia Guice
Dr. Anne Hughes
Dr. Buchele
Dr. Clark
Dr. Harvey
Dr. John Labban
Dr. John Suen
Dr. Puleo
Dr. Rajesh Rana
Dr. Rustagi
Dr. Schermerhorn
Dr. Shah
Ear, Nose & Throat Associates, P.C.
East Carolina Medical Associates
Eastern Washington Dermatology Associates
Ellinwood District Hospital
Family Care Chiropractic Center
Family Practice Associates of Macomb
Family Practice of Macomb
Floyd Trillis Jr., M.D.
Fredonia Regional Hospital
Fremont Family Medicine
Generations Primary Care
Grace Community Health Center, Inc.
Grisell Memorial Hospital
Harding Pediatrics LLP
Harlan County Health System
Health Access Program
Heart Institute of Venice
Henderson Minor Outpatient Medicine
Henry County Hospital myhealth portal
Highgate Clinic
Hobart Family Medical Clinic
Howard Stierwalt, M.D.
Howard University Hospital
Hudson Essex Nephrology
Huntington Medical Associates
Huntington Medical Group
Hutchinson Regional Medical Center
Idaho Sports Medicine Institute
In Step Foot & Ankle Specialists
Independence Rehabilitation Inc
Indiana Endocrine Specialists
Indiana Internal Medicine Consultants
Indiana Ohio Heart
Indiana Surgical Specialists
Indiana University
Indiana University Health Center
Indianapolis Gastroenterology and Hepatology
Internal Medicine Associates
IU - Northwest
Jackson Neurolosurgery Clinic
James E. Hunt, MD
Jasmine K. Leong MD
Jewell County Hospital
John Hiestand, M.D.
Jonathan F. Diller, M.D.
Jubilee Community Health
Kardous Primary Care
Keith A. Harvey, M.D.
Kenneth Cesa DPM
Kings Clinic and Urgent Care
Kiowa County Memorial Hospital
Kristin Egan MD
Lakeshore Family Practice
Lane County Hospital
Logan County Hospital
Margaret Mary Health
Masonboro Urgent Care
McDonough Medical Group Psychiatry
Medical Care, Inc.
Medical Center of East Houston
Medicine Lodge Memorial Hospital
MedPartners

MHP Cardiology
Michael Mann, MD, PC
Michelle Barnes Marshall, P.C.
Michiana Gastroenterology, Inc.
Minneola District Hospital
Mora Surgical Clinic
Moundridge Mercy Hospital Inc
myhealthnow
Nancy L. Carteron M.D.
Naples Heart Rhythm Specialists
Nate Delisi DO
Neighborhood Health Clinic
Neosho Memorial Regional Medical Center
Neuro Spine Pain Surgery Center
Norman G. McKoy, M.D. & Ass., P.A.
North Corridor Internal Medicine
Nova Pain Management
Novapex Franklin
Oakland Family Practice
Oakland Medical Group
Ohio Physical Medicine & Rehabilitation Inc.
On Track For Life
Ottawa County Health Center
Pareshchandra C. Patel MD
Parkview Health System, Inc. d/b/a Family Practice Associates of Huntington
Parkview Health System, Inc. d/b/a Fort Wayne Cardiology
Parrott Medical Clinic
Partners In Family Care
Personalized Health Care Of Tucson
Phillips County Hospital
Physical Medicine Consultants
Physicians of North Worchester County
Precision Weight Loss Center
Primary & Alternative Medical Center
Prince George's County Health Department
Rebecca J. Kurth M.D.
Relief Center
Republic County Hospital
Ricardo S. Lemos MD
Richard A. Stone M.D.
Richard Ganz MD
River Primary Care
Rolando P. Oro MD, PA
Ronald Chochinov
Sabetha Community Hospital
Santa Cruz Pulmonary Medical Group
Santone Chiropractic
Sarasota Cardiovascular Group
Sarasota Center for Family Health Wellness
Sarasota Heart Center
Satanta District Hospital
Saul & Cutarelli MD's Inc.
Shaver Medical Clinic, P. A.
Skiatook Osteopathic Clinic Inc.
Sleep Centers of Fort Wayne
Smith County Hospital
Smith Family Chiropractic
Somers Eye Center
South Forsyth Family Medicine & Pediatrics
Southeast Rehabilitation Associates PC
Southgate Radiology
Southwest Internal Medicine & Pain Management
Southwest Orthopaedic Surgery Specialists,PLC
Stafford County Hospital
Stephen Helvie MD
Stephen T. Child MD
Susan A. Kubica MD
Texas Childrens Hospital
The Children's Health Place
The Heart & Vascular Specialists
The Heart and Vascular Center of Sarasota
The Imaging Center
The Johnson Center for Pelvic Health
The Medical Foundation, My Lab Results Portal
Thompson Family Chiropractic
Trego County Hospital
Union Square Dermatology
Volunteers in Medicine
Wells Chiropractic Clinic
Wichita County Health Center
William Klope MD
Wyoming Total Health Record Patient Portal
Yovanni Tineo M.D.
Zack Hall M.D.

In addition to its previously identified clients, the following additional healthcare providers were affected by the Medical Informatics Engineering cyber attack. Patients of these healthcare providers may be affected, and individual notice letters have been sent to affected individuals for whom we have a valid mailing address. Affected healthcare providers include:

RediMed

Allied Physicians, Inc. d/b/a Fort Wayne Neurological Center (including Neurology, Physical Medicine and Neurosurgery)
Fort Wayne Radiology Association, LLC including d/b/a Nuvena Vein Center and Dexa Diagnostics
Open View MRI, LLC
Breast Diagnostic Center, LLC
P.E.T. Imaging Services, LLC
MRI Center -Fort Wayne Radiology, Inc. (f/k/a Advanced Imaging Systems, Inc.)

Individuals who received services from Fort Wayne Radiology Association, Open View, Breast Diagnostic Center, PET Imaging or MRI Center during the period of time from January 1, 1997 to May 26, 2015 may be affected. The database relating to these healthcare providers was accessed on May 26, 2015. Individuals may also visit the providers' websites, which may be accessed at www.fwradiology.com , for information on this incident. Affected individuals may include, along with potential others, individuals who received radiology services during this time at any of the organizations identified below:

Accustat Medical Lab, Inc.	Indianapolis, IN
Allergy & Asthma Center	Fort Wayne, IN
Associated Physicians & Surgeons Clinic, LLC	Terre Haute, IN
Ball Memorial Hospital	Muncie, IN
Bedford Regional Medical Center	Bedford, IN
Cameron Memorial Community Hospital	Angola, IN
Central Indiana Orthopedics, PC	Muncie, IN
Community Memorial Hospital	Hicksville, OH
Ear, Nose & Throat Associates	Fort Wayne, IN
Family Medicine Associates, Jerry Sell, M.D.	Rockford, OH
First Care Family Physicians	Fort Wayne, IN
Fort Wayne Medical Oncology & Hematology	Fort Wayne, IN
Gary Pitts, M.D.	Warsaw, IN
Indiana Urgent Care Centers, LLC	Indianapolis, IN
Indiana University Health Center	Bloomington, IN
Jasper County Hospital	Rensselaer, IN
Manchester Family Physicians	North Manchester, IN
MedCorp	Toledo, OH
Meridian Health Group	Carmel, IN
Nationwide Mobile Imaging	Fort Wayne, IN
Neighborhood Health Clinic	Fort Wayne, IN
Orthopaedics Northeast	Fort Wayne, IN
Parkview Regional Medical Center	Fort Wayne, IN
Parkview Hospital	Fort Wayne, IN
Parkview Ortho Hospital	Fort Wayne, IN
Parkview Heart Institute	Fort Wayne, IN
Parkview Women & Children's Hospital	Fort Wayne, IN
Parkview Noble Hospital	Kendallville, IN
Parkview Huntington Hospital	Huntington, IN
Parkview Whitley Hospital	Columbia City, IN
Parkview LaGrange Hospital	LaGrange, IN
Parkview Physicians Group	
Parkview Occupational Health Centers	
Paulding County Hospital	Paulding, OH
Prompt Care Express	Coldwater, MI; Sturgis, MI
Public Safety Medical Services	Indianapolis, IN
Purdue University Health Center	W. Lafayette, IN
Southwestern Medical Clinics	Berrien Springs, MI

Tri-State Medical Imaging	Angola, Indiana
Union Associated Physicians Clinic	Terre Haute, IN
U.S. Healthworks Medical Group of Indiana	Elkhart, IN
Van Wert County Hospital	Van Wert, OH
Wabash County Hospital	Wabash, IN
Wabash Family Care	Wabash, IN

We take the security of health information very seriously and understand that such incidents cause real concern. We apologize sincerely and thank our customers for their continued loyalty and patience as we work through this challenge.

Medical Informatics Engineering Updates Notice to Individuals of a Data Security Compromise

Fort Wayne, Indiana, July 23, 2015 Medical Informatics Engineering is providing an update to our June 10, 2015 notice of a data security compromise that has affected the security of some personal and protected health information relating to certain clients and individuals who have used a Medical Informatics Engineering electronic health record. *We emphasize that the patients of only certain clients of Medical Informatics Engineering were affected by this compromise and those clients have all been notified.*

On May 26, 2015, we discovered suspicious activity in one of our servers. We immediately began an investigation to identify and remediate any identified security vulnerability. Our first priority was to safeguard the security of personal and protected health information, and we have been working with a team of third-party experts to investigate the attack and enhance data security and protection. This investigation is ongoing. On May 26, 2015, we also reported this incident to law enforcement including the FBI Cyber Squad. Law enforcement is actively investigating this matter, and we are cooperating fully with law enforcement's investigation. The investigation indicates this is a sophisticated cyber attack. Our forensic investigation indicates the unauthorized access to our network began on May 7, 2015. Our monitoring systems helped us detect this unauthorized access, and we were able to shut down the attackers as they attempted to access client data.

We are continuing to take steps to remediate and enhance the security of our systems. Remedial efforts include removing the capabilities used by the intruder to gain unauthorized access to the affected systems, enhancing and strengthening password rules and storage mechanisms, increased active monitoring of the affected systems, and intelligence exchange with law enforcement. We have also instituted a universal password reset.

Information compromised

While investigations into this incident are ongoing, we determined the security of some personal and protected health information contained on Medical Informatics Engineering's network has been affected. The affected data relating to individuals affiliated with affected Medical Informatics Engineering clients may include an individual's name, telephone number, mailing address, username, hashed password, security question and answer, spousal information (name and potentially date of birth), email address, date of birth, Social Security number, lab results, health insurance policy information, diagnosis, disability code, doctor's name, medical conditions, and child's name and birth statistics.

Notification

On June 2, 2015, we began contacting and mailing notice letters disclosing this incident to affected Medical Informatics Engineering clients.

On July 17, 2015, we began mailing notice letters to affected individuals for whom we have a valid postal address through U.S. mail, and we expect those letters to be mailed on or before July 25, 2015. Information contained in the notice letter is available at www.mieweb.com. We have also disclosed this incident to certain state and federal regulators and to the consumer reporting agencies.

Identity protection services

As the investigations continue, and out of an abundance of caution, we are offering affected individuals access to two years of credit monitoring and identity protection services at no cost.

Fraud prevention tips

We suggest affected individuals remain vigilant and seek to protect against possible identity theft or other financial loss by regularly reviewing their financial account statements for suspicious activity. We also encourage affected individuals to notify their credit card companies, health care providers, and heath care insurers of this data security incident. Affected individuals may also review explanation of benefits statement(s) that they receive from their healthcare provider or health plan. If an affected individual sees any service that he/she believes he/she did not receive, the individual should contact his/her health care provider or health plan at the telephone number listed on the explanation of benefits statement(s). If an affected individual does not receive regular explanation of benefits statement(s), we suggest he/she contact his/her healthcare provider or health plan and ask that they send a copy after each visit the affected individual makes with his/her health care provider.

We also suggest that affected individuals carefully review their credit reports. Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, visit www.annualcreditreport.com or call, toll-free, (877) 322-8228.

At no charge, individuals can also have these credit bureaus place a "fraud alert" on their file that alerts creditors to take additional steps to verify the his/her identity prior to granting credit in his/her name. Please note, however, that because it tells creditors to follow certain procedures to protect an individual's credit, it may also delay the ability to obtain credit while the agency verifies the individual's identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on an individual's file. If you wish to place a fraud alert, or you have questions regarding your credit report, you can contact any one of the following agencies: **Equifax**, Consumer Fraud Division, P.O. Box 740256, Atlanta, GA 30374, (800) 525-6285, www.equifax.com; **Experian**, Consumer Fraud Assistance, P.O. Box 9556, Allen, TX 75013, (888) 397-3742, www.experian.com; **TransUnion**, Consumer Relations & Fraud Victim Assistance, 1561 E. Orangethorpe Avenue, Fullerton, CA 92831, (800) 372-8391, www.transunion.com. Information regarding security freezes may also be obtained from these sources.

The Federal Trade Commission (FTC) encourages those who discover that their information has been misused to file a complaint with them. To file a complaint with the FTC, or to obtain additional information on identity theft and the steps that can be taken to avoid identity theft, the FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, www.ftc.gov/idtheft, (877) ID-THEFT (877-438-4338); TTY: (866) 653-4261. This notice has not been delayed because of law enforcement; however, instances of known or suspected identity theft should be reported to local law enforcement, your state Attorney General, and the FTC. State Attorneys General may also have advice on preventing identity theft. Individuals can also learn more about placing a fraud alert or security freeze on their credit files by contacting the FTC or state Attorney General. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us. For Kentucky residents, the Attorney General can be contacted at 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601-3449, 502-696-5389, www.ag.ky.gov. For Indiana residents, the Attorney General can be contacted at 302 W. Washington Street, Indianapolis, Indiana 46204, (317) 232-6201, www.in.gov.

Security Freeze

Under MA and WV law, affected individuals have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Under MA and WV law, you may place a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without your written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services.

If you have been a victim of identity theft, and provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 in MA and $5.30 in WV each to place, temporarily lift, or permanently remove a security freeze. To place a

security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving a request to place a security freeze on a credit file report. The credit bureaus must also send written confirmation to the individual within five (5) business days and provide individual with a unique personal identification number (PIN) or password, or both, that can be used to authorize the removal or lifting of the security freeze. To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to remove the security freeze.

Toll-free hotline

We have established a confidential, toll free hotline to assist affected individuals with questions regarding the incident, their affected personal and protected health information, their affected healthcare provider(s), and the identity monitoring and protection services we are making available. The hotline can be reached at (866) 328-1987, Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time, except for holidays. If you would like to confirm whether you are affected by this incident, you may call our hotline. Updates regarding this incident, our investigation and steps individuals may take to protect themselves from identity theft and fraud will be available on www.mieweb.com and through our toll free hotline. Questions regarding the incident should not be directed to your healthcare provider(s) as they may not be able to answer your questions.

Affected entities

The following healthcare providers were affected by the Medical Informatics Engineering cyber attack. Patients of these healthcare providers may be affected, and individual notice letters have been sent to affected individuals for whom we have a valid mailing address. Affected healthcare providers include:

Concentra
Allied Physicians, Inc. d/b/a Fort Wayne Neurological Center (including Neurology, Physical Medicine and Neurosurgery)
Franciscan St. Francis Health Indianapolis
Gynecology Center, Inc. Fort Wayne
Rochester Medical Group
RediMed
Fort Wayne Radiology Association, LLC including d/b/a Nuvena Vein Center and Dexa Diagnostics
Open View MRI, LLC
Breast Diagnostic Center, LLC

P.E.T. Imaging Services, LLC
MRI Center -Fort Wayne Radiology, Inc. (f/k/a Advanced Imaging Systems, Inc.)

Individuals who received services from Fort Wayne Radiology Association, Open View, Breast Diagnostic Center, PET Imaging or MRI Center during the period of time from January 1, 1997 to May 26, 2015 may be affected. The database relating to these healthcare providers was accessed on May 26, 2015. Individuals may also visit the providers' websites, which may be accessed at www.fwradiology.com , for information on this incident. Affected individuals may include, along with potential others, individuals who received radiology services during this time at any of the organizations identified below:

Accustat Medical Lab, Inc.	Indianapolis, IN
Allergy & Asthma Center	Fort Wayne, IN
Associated Physicians & Surgeons Clinic, LLC	Terre Haute, IN
Ball Memorial Hospital	Muncie, IN
Bedford Regional Medical Center	Bedford, IN
Cameron Memorial Community Hospital	Angola, IN
Central Indiana Orthopedics, PC	Muncie, IN
Community Memorial Hospital	Hicksville, OH
Ear, Nose & Throat Associates	Fort Wayne, IN
Family Medicine Associates, Jerry Sell, M.D.	Rockford, OH
First Care Family Physicians	Fort Wayne, IN
Fort Wayne Medical Oncology & Hematology	Fort Wayne, IN
Gary Pitts, M.D.	Warsaw, IN
Indiana Urgent Care Centers, LLC	Indianapolis, IN
Indiana University Health Center	Bloomington, IN
Jasper County Hospital	Rensselaer, IN
Manchester Family Physicians	North Manchester, IN
MedCorp	Toledo, OH
Meridian Health Group	Carmel, IN
Nationwide Mobile Imaging	Fort Wayne, IN
Neighborhood Health Clinic	Fort Wayne, IN
Orthopaedics Northeast	Fort Wayne, IN
Parkview Regional Medical Center	Fort Wayne, IN
Parkview Hospital	Fort Wayne, IN
Parkview Ortho Hospital	Fort Wayne, IN
Parkview Heart Institute	Fort Wayne, IN
Parkview Women & Children's Hospital	Fort Wayne, IN
Parkview Noble Hospital	Kendallville, IN
Parkview Huntington Hospital	Huntington, IN
Parkview Whitley Hospital	Columbia City, IN
Parkview LaGrange Hospital	LaGrange, IN
Parkview Physicians Group	
Parkview Occupational Health Centers	
Paulding County Hospital	Paulding, OH
Prompt Care Express	Coldwater, MI; Sturgis, MI
Public Safety Medical Services	Indianapolis, IN
Purdue University Health Center	W. Lafayette, IN
Southwestern Medical Clinics	Berrien Springs, MI
Tri-State Medical Imaging	Angola, Indiana
Union Associated Physicians Clinic	Terre Haute, IN
U.S. Healthworks Medical Group of Indiana	Elkhart, IN
Van Wert County Hospital	Van Wert, OH

Wabash County Hospital	Wabash, IN
Wabash Family Care	Wabash, IN

We take the security of health information very seriously and understand that such incidents cause real concern. We apologize sincerely and thank our customers for their continued loyalty and patience as we work through this challenge.

NoMoreClipboard Updates Notice to Individuals of a Data Security Compromise

Fort Wayne, Indiana, July 23, 2015 On behalf of itself and its affected clients, NoMoreClipboard is updating its June 10, 2014 notice of a data security compromise that has affected the security of some personal and protected health information relating to individuals who have used a NoMoreClipboard personal health record or patient portal. *We emphasize that the affected NoMoreClipboard clients have been notified of this data security compromise.*

On May 26, 2015, we discovered suspicious activity in one of our servers. We immediately began an investigation to identify and remediate any identified security vulnerability. Our first priority was to safeguard the security of personal and protected health information, and we have been working with a team of third-party experts to investigate the attack and enhance data security and protection. This investigation is ongoing. On May 26, 2015, we also reported this incident to law enforcement including the FBI Cyber Squad. Law enforcement is actively investigating this matter, and we are cooperating fully with law enforcement's investigation. The investigation indicates this is a sophisticated cyber attack. Our forensic investigation indicates the unauthorized access to our network began on May 7, 2015. Our monitoring systems helped us detect this unauthorized access, and we were able to shut down the attackers as they attempted to access client data.

We are continuing to take steps to remediate and enhance the security of our systems. Remedial efforts include removing the capabilities used by the intruder to gain unauthorized access to the affected systems, enhancing and strengthening password rules and storage mechanisms, increased active monitoring of the affected systems, and intelligence exchange with law enforcement. We have also instituted a universal password reset.

Information compromised

While investigations into this incident are ongoing, we determined the security of some personal and protected health information contained on Medical Informatics Engineering's network has been affected. The affected data relating to individuals who used a NoMoreClipboard portal/personal health record may include an individuals' name, home address, Social Security number, username, hashed password, spousal information (name and potentially date of birth), security question and answer, email address, date of birth, health information, and health insurance policy information.

Notification

On June 2, 2015, we began contacting and mailing notice letters disclosing this incident to affected NoMoreClipboard clients.

On July 17, 2015, we began mailing notice letters to affected individuals for whom we have a valid postal address through U.S. mail, and we expect those letters to be mailed on or before July 25, 2015. Information contained in the notice letter is available at www.NoMoreClipboard.com. We have also disclosed this incident to certain state and federal regulators and to the consumer reporting agencies.

Identity protection services

As the investigations continue, and out of an abundance of caution, we are offering affected individuals access to two years of credit monitoring and identity protection services at no cost.

Fraud prevention tips

We suggest affected individuals remain vigilant and seek to protect against possible identity theft or other financial loss by regularly reviewing their financial account statements for suspicious activity. We also encourage affected individuals to notify their credit card companies, health care providers, and heath care insurers of this data security incident. Affected individuals may also review explanation of benefits statement(s) that they receive from their healthcare provider or health plan. If an

affected individual sees any service that he/she believes he/she did not receive, the individual should contact his/her health care provider or health plan at the telephone number listed on the explanation of benefits statement(s). If an affected individual does not receive regular explanation of benefits statement(s), we suggest he/she contact his/her healthcare provider or health plan and ask that they send a copy after each visit the affected individual makes with his/her health care provider.

We also suggest that affected individuals carefully review their credit reports. Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, visit www.annualcreditreport.com or call, toll-free, (877) 322-8228.

At no charge, individuals can also have these credit bureaus place a "fraud alert" on their file that alerts creditors to take additional steps to verify the his/her identity prior to granting credit in his/her name. Please note, however, that because it tells creditors to follow certain procedures to protect an individual's credit, it may also delay the ability to obtain credit while the agency verifies the individual's identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on an individual's file. If you wish to place a fraud alert, or you have questions regarding your credit report, you can contact any one of the following agencies: **Equifax**, Consumer Fraud Division, P.O. Box 740256, Atlanta, GA 30374, (800) 525-6285, www.equifax.com; **Experian**, Consumer Fraud Assistance, P.O. Box 9556, Allen, TX 75013, (888) 397-3742, www.experian.com; **TransUnion**, Consumer Relations & Fraud Victim Assistance, 1561 E. Orangethorpe Avenue, Fullerton, CA 92831, (800) 372-8391, www.transunion.com. Information regarding security freezes may also be obtained from these sources.

The Federal Trade Commission (FTC) encourages those who discover that their information has been misused to file a complaint with them. To file a complaint with the FTC, or to obtain additional information on identity theft and the steps that can be taken to avoid identity theft, the FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, www.ftc.gov/idtheft, (877) ID-THEFT (877-438-4338); TTY: (866) 653-4261. This notice has not been delayed because of law enforcement; however, instances of known or suspected identity theft should be reported to local law enforcement, your state Attorney General, and the FTC. State Attorneys General may also have advice on preventing identity theft. Individuals can also learn more about placing a fraud alert or security freeze on their credit files by contacting the FTC or state Attorney General. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us. For Kentucky residents, the Attorney General can be contacted at 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601-3449, 502-696-5389, www.ag.ky.gov. For Indiana residents, the Attorney General can be contacted at 302 W. Washington Street, Indianapolis, Indiana 46204, (317) 232-6201, www.in.gov.

Security Freeze

Under MA and WV law, affected individuals have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Under MA and WV law, you may place a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without your written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services.

If you have been a victim of identity theft, and provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 in MA and $5.30 in WV each to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over

the prior five years;

5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving a request to place a security freeze on a credit file report. The credit bureaus must also send written confirmation to the individual within five (5) business days and provide individual with a unique personal identification number (PIN) or password, or both, that can be used to authorize the removal or lifting of the security freeze. To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to remove the security freeze.

Toll-free hotline

We have established a confidential, toll free hotline to assist affected individuals with questions regarding the incident, their affected personal and protected health information, their affected healthcare provider(s), and the identity monitoring and protection services we are making available. The hotline can be reached at (866) 328-1987, Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time, except for holidays. If you would like to confirm whether you are affected by this incident, you may call our hotline. Updates regarding this incident, our investigation and steps individuals may take to protect themselves from identity theft and fraud will be available on www.nomoreclipboard.com and through our toll free hotline. Questions regarding the incident should not be directed to your healthcare provider(s) as they may not be able to answer your questions.

Affected entities

Physician practices, hospitals, and other organizations work with NoMoreClipboard to offer patient portals and personal health records which enable consumers to access and manage health information online. Individuals who use patient portals or personal health records offered by the following entities may be affected by this cyber attack. Individual notice letters have been sent to affected individuals for whom we have a valid mailing address. Affected organizations include:

Advanced Cardiac Care
Advanced Foot Specialists
All About Childrens Pediatric Partners, PC
Allen County Dept of Health
Allied Physicians, Inc. d/b/a Fort Wayne Neurological Center (including Neurology, Physical Medicine and Neurosurgery)
Altagracia Medical Center
Anderson Family Medicine
Arkansas Otolaryngology, P.A.
Auburn Cardiology Associates
Basedow Family Clinic Inc.
Bastrop Medical Clinic
Batish Family Medicine
Beaver Medical
Boston Podiatry Services PC
Brian Griner M.D.
Brightstarts Pediatrics
Burnsville Medical Center
Capital Rehabilitation
Cardiovascular Consultants of Kansas
Carl Gustafson OD
Carolina Gastroenterology
Carolina Kidney & Hypertension Center
Carolinas Psychiatric Associates
Center for Advanced Spinal Surgery
Chang Neurosurgery & Spine Care
Cheyenne County Hospital
Children's Clinic of Owasso, P.C.
Clara A. Lennox MD
Claude E. Younes M.D., Inc.
CMMC

Coalville Health Center
Cornerstone Medical and Wellness, LLC
Cumberland Heart
David A. Wassil, D.O.
David M Mayer MD
Dr. Alicia Guice
Dr. Anne Hughes
Dr. Buchele
Dr. Clark
Dr. Harvey
Dr. John Labban
Dr. John Suen
Dr. Puleo
Dr. Rajesh Rana
Dr. Rustagi
Dr. Schermerhorn
Dr. Shah
Ear, Nose & Throat Associates, P.C.
East Carolina Medical Associates
Eastern Washington Dermatology Associates
Ellinwood District Hospital
Family Care Chiropractic Center
Family Practice Associates of Macomb
Family Practice of Macomb
Floyd Trillis Jr., M.D.
Fredonia Regional Hospital
Fremont Family Medicine
Generations Primary Care
Grace Community Health Center, Inc.
Grisell Memorial Hospital
Harding Pediatrics LLP
Harlan County Health System
Health Access Program
Heart Institute of Venice
Henderson Minor Outpatient Medicine
Henry County Hospital myhealth portal
Highgate Clinic
Hobart Family Medical Clinic
Howard Stierwalt, M.D.
Howard University Hospital
Hudson Essex Nephrology
Huntington Medical Associates
Huntington Medical Group
Hutchinson Regional Medical Center
Idaho Sports Medicine Institute
In Step Foot & Ankle Specialists
Independence Rehabilitation Inc
Indiana Endocrine Specialists
Indiana Internal Medicine Consultants
Indiana Ohio Heart
Indiana Surgical Specialists
Indiana University
Indiana University Health Center
Indianapolis Gastroenterology and Hepatology
Internal Medicine Associates
IU - Northwest
Jackson Neurolosurgery Clinic
James E. Hunt, MD
Jasmine K. Leong MD
Jewell County Hospital
John Hiestand, M.D.
Jonathan F. Diller, M.D.
Jubilee Community Health
Kardous Primary Care
Keith A. Harvey, M.D.
Kenneth Cesa DPM
Kings Clinic and Urgent Care
Kiowa County Memorial Hospital
Kristin Egan MD
Lakeshore Family Practice
Lane County Hospital
Logan County Hospital
Margaret Mary Health
Masonboro Urgent Care
McDonough Medical Group Psychiatry
Medical Care, Inc.
Medical Center of East Houston
Medicine Lodge Memorial Hospital
MedPartners
MHP Cardiology
Michael Mann, MD, PC
Michelle Barnes Marshall, P.C.
Michiana Gastroenterology, Inc.
Minneola District Hospital
Mora Surgical Clinic
Moundridge Mercy Hospital Inc
myhealthnow
Nancy L. Carteron M.D.
Naples Heart Rhythm Specialists
Nate Delisi DO
Neighborhood Health Clinic
Neosho Memorial Regional Medical Center
Neuro Spine Pain Surgery Center
Norman G. McKoy, M.D. & Ass., P.A.
North Corridor Internal Medicine
Nova Pain Management
Novapex Franklin
Oakland Family Practice
Oakland Medical Group
Ohio Physical Medicine & Rehabilitation Inc.
On Track For Life
Ottawa County Health Center

Pareshchandra C. Patel MD
Parkview Health System, Inc. d/b/a Family Practice Associates of Huntington
Parkview Health System, Inc. d/b/a Fort Wayne Cardiology
Parrott Medical Clinic
Partners In Family Care
Personalized Health Care Of Tucson
Phillips County Hospital
Physical Medicine Consultants
Physicians of North Worchester County
Precision Weight Loss Center
Primary & Alternative Medical Center
Prince George's County Health Department
Rebecca J. Kurth M.D.
Relief Center
Republic County Hospital
Ricardo S. Lemos MD
Richard A. Stone M.D.
Richard Ganz MD
River Primary Care
Rolando P. Oro MD, PA
Ronald Chochinov
Sabetha Community Hospital
Santa Cruz Pulmonary Medical Group
Santone Chiropractic
Sarasota Cardiovascular Group
Sarasota Center for Family Health Wellness
Sarasota Heart Center
Satanta District Hospital
Saul & Cutarelli MD's Inc.
Shaver Medical Clinic, P. A.
Skiatook Osteopathic Clinic Inc.
Sleep Centers of Fort Wayne
Smith County Hospital
Smith Family Chiropractic
Somers Eye Center
South Forsyth Family Medicine & Pediatrics
Southeast Rehabilitation Associates PC
Southgate Radiology
Southwest Internal Medicine & Pain Management
Southwest Orthopaedic Surgery Specialists,PLC
Stafford County Hospital
Stephen Helvie MD
Stephen T. Child MD
Susan A. Kubica MD
Texas Childrens Hospital
The Children's Health Place
The Heart & Vascular Specialists
The Heart and Vascular Center of Sarasota
The Imaging Center
The Johnson Center for Pelvic Health
The Medical Foundation, My Lab Results Portal
Thompson Family Chiropractic
Trego County Hospital
Union Square Dermatology
Volunteers in Medicine
Wells Chiropractic Clinic
Wichita County Health Center
William Klope MD
Wyoming Total Health Record Patient Portal
Yovanni Tineo M.D.
Zack Hall M.D.

We take the security of health information very seriously and understand that such incidents cause real concern. We apologize sincerely and thank our customers for their continued loyalty and patience as we work through this challenge.